INTERNATIONAL
HELLENIC
UNIVERSITY

An analysis and a web based wizard-like decision support system to countermeasure electronic surveillance

Ioannis Papakyriazis

SID: 3301110016

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

DECEMBER 2013

THESSALONIKI – GREECE

An analysis and a web based wizard-like decision support system to countermeasure electronic surveillance

Ioannis Papakyriazis

SID: 3301110016

Supervisor:	Prof. Vasileios Katos
Supervising Committee Members:	Assoc. Prof. Name Surname
	Assist. Prof. Name Surname

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

DECEMBER 2013

THESSALONIKI – GREECE

Abstract

The topic of online privacy, seen as an extremely valuable but endangered commodity is analyzed within the scope of recent developments.

Online privacy is a fundamental right of every individual, but at the same time it is not easily defined or borderlined. As a result, it is under permanent threat for violation and given the latest surveillance facts is one of the topics on top of the list of global interest for more awareness and transparency.

The main thesis of this project is that individual users should try to keep an acceptable level of privacy by applying practices that help him be as immune as possible to both state and corporate arbitrariness.

After a n extensive literature review of surveillance, privacy and notions about modern state and corporate monitoring, the key theories of technology acceptance are analyzed and some modifications are proposed for connecting social psychology with tangible results, with the use of some privacy and technology competence related survey tools.
The results of those tools are then analyzed to drive to the practical part of the project, which is a simple wizard-like decision support system that helps the individual achieve the maximum possible personal level of privacy, regarding his technology level and habits.
Following this work, a number of additions should be applied so that it best integrates to the future nature of online security problems related to the topic.

Keywords: Privacy, surveillance, security, NSA, Technology Acceptance Model, questionnaire, countermeasures, wizard, proposals

Acknowledgments:

I would like to thank my supervisor Vasilis Katos for his guidance throughout this process.

Special thanks to my friend Christina Sereti for her ideas and a technical aid of this work.

Ioannis Papakyriazis

4.12.2013

Contents

1 Introduction

This dissertation is about the highly topical subject of information systems surveillance. It is seen by the perspective of an average internet user, who is overwhelmed by currently flowing information on the latest US National Security Agency scandal - a multinational espionage thriller involving governments, secret agencies, internet companies and so forth. Terms with negative aspect such as privacy violation, surveillance, wiretapping, monitoring, control, eavesdropping, snooping and many more appear frequently in the media, causing potential unrest and confusion to people eventually affecting their judgment when being online and performing transactions.

The goal of the thesis is to shed some light on the current implications of electronic privacy and propose a number of practices for securing online presence, to the best extent, without burdening typical users with unsuitable applications.

The objectives of the thesis are

(1) to raise awareness about the problem of electronic privacy,

(2) to incorporate new determinants of technology acceptance in widely recognized theoretical models and

(3) to apply a simple yet helpful decision support system to reach the goal mentioned above.

1.1 Motivation

On an grim article by Rick Falkvinge on Infopolicy, [1] "The night of June 6, 2013, the news detonated that the USA's National Security Agency (NSA) has had direct access to almost every mainstream social network for the past several years, dating back to 2007, under a program named PRISM. Under this framework" - studied later on this paper- "a number of social network services feed people's private data to the NSA. In short, if somebody has been using/uploading:

E-mail, video or voice or text chat, videos, photos, stored data, VoIP calls, file transfers, video conferencing (and more) from any of:

- Microsoft, since Sep 2007
- Google, since Jan 2009
- Yahoo, since Mar 2008
- Facebook, since June 2009
- PalTalk, since Dec 2009
- YouTube, since Sep 2010

- Skype, since Feb 2011
- AOL, since Mar 2011,
- Apple, since Oct 2012

then he is most probably been continuously wiretapped".

These news was not so much of a surprise to IS security experts worldwide who always suspected and warned the community about similar activities, but for sure it's a different thing when such extraordinary amount of classified information come to light.

As this was not bad enough, New York Times proceed to new revelations about NSA: "The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated."[2]

In short, this allegation means that besides the capability of eavesdropping (of virtually the entire Internet), the cryptography of commercial software is compromised through deliberately planted vulnerabilities (back doors), in collaboration with the companies who implemented it. The proof, as we are going to meet later (§2.2) on this essay, are too many and too obvious to overlook.

So, as the ease and density of use of technology accelerates, so does the surveillance and anti-privacy tools, thus the challenge for users to be more informed and protected *rises*.

This struggle was important enough to 30-year-old former N.S.A. contractor *Edward Snowden* [3] to become a "whistleblower" and give up his life, career, and temporarily (?) his freedom, leaking to the "Guardian" and the "Washington Post" previously undisclosed programs to monitor telephone and internet traffic.

Despite this, on a "Scandal Of The Summer" August 2013 poll by Harris Interactive [4] even though seven in ten Americans say they have paid attention to the Snowden scandal, and although nearly half of them (47%) agree that he was brave to expose the surveillance programs to the world, four in ten (39%) disagree and 14% are not at all sure.

That result, even if it is rather not unexpected coming from American citizens' opinions, could be seen as a motivation for this study. Much more awareness is needed in order to understand the key concept of *privacy versus ease of use* and moreover, a big effort is required to draw conclusions as to what a single everyday internet user should do in order to counter the undesired effects of online surveillance.

1.2 Rise of a new era of surveillance

The amazing gifts of the internet that the world came to uncritically adore and depend upon from the 1990's are now starting to reveal another side.

Nation states have adopted to the new technology reality by building an infrastructure that can almost automatically be reused to control the public. The nature of current technology requires that public data are either totally secure, or totally insecure in a way that enables the widespread and exhaustive monitoring of whole populations. State surveillance also has a long history of suppressing social movements, which chill down by extensive monitoring.

Corporations on the other hand are obliged to harvest and analyze massive amounts of personal data in order to remain competitive in our information-flooded world. This is to say, nearly all online advertising is shifting towards surveillance-based tracking of our personal electronic habits. Those enormous amounts of mined data not only give corporations exceptional power over customers, but can also be directly reused by authorities.

Those two stakeholders of *the Information Snooperhighway,*[1] as defined in "The Electronic Privacy Papers" book [5] seem to dominate via todays network infrastructure and services in unprecedented ways. . In other words, corporations follow business models that treat customer privacy as a free profit-making resource while at the same time state exploits citizens data for several nebulous reasons.

Reviewing the literature we meet J. Gilliom's assessment: "In today's seamless electronic environment, both private corporations and government agencies take advantage of the powerful technological surveillance means to track and profile consumers and citizens. These profiles could be used to acquire knowledge about individual preferences and behaviors, for marketing purposes and for the prevention and detection of cyber-attacks, fraud and other crimes, as well as terrorist activities" [6]

When people start to learn about this rise in surveillance they start to feel frustrated.

- A part of people decide it is impossible to keep their privacy, so they let themselves live under permanent surveillance

[1] Pun intended , snooperhighway instead of the mainstream "superhighway" of information, i.e. the Internet

- Some others try to learn how to defend themselves from being spied on, but find it very difficult to put all the time and effort to be up-to-date and efficient into avoiding it
- Few, *Digerati* (word is a blend of 'digital' and 'literati', means collectively people who are considered the *elite* -for whatever reason- in information technology [7]) manage to keep a good level of personal privacy online
- Finally a big proportion of the population embraces the new reality and willingly participates in any new social networking application by flooding the internet with all kinds of personal data, establishing the new "nothing to hide" trend. They voluntarily log their whole life, recording almost everything they do and placing it straight online in real-time. So, what was a subculture some years ago has now become mainstream.

From morning till bed time at night, people leave trails of data behind them for others to collect, analyze, process and eventually sell to advertising companies, usually without their knowledge, their consent or both.

1.3 Roadmap

The study proceeds following the format described here:

Chapter 2 starts with a literature review, where the definitions and notions of *security, surveillance* and other related contexts are examined; the modern surveillance frameworks are described, followed by some new countermeasure approaches.

We then present the most dominant theoretical models of *technology acceptance*, which will be tweaked to serve the purpose of the practical part of this dissertation.

On chapter 3 we define the problem of the *security versus privacy balance* and introduce the proposed variants to the models mentioned above, establishing the theoretical contribution of this work; the next step is to obtain primary data via some questionnaires, in order to analyze and interpret the results so far.

On chapter 4 we design and implement the system that classifies users' needs for privacy and proposes existing/running/tested/ alternatives for common applications that are on stake for data privacy issues.

Finally on chapter 5 we conclude our findings, and suggest future improvements and modifications to the work done.

2 Literature review

In this chapter, we first research some basic constructs of the *surveillance and privacy* context, followed by some interesting numeric facts. Following this, we define the concept of *metadata* and how the modern surveillance programs take advantage of them. Consequently, some countermeasure approaches follow.

The next part of the research is dealing with a whole different context, the *technology acceptance* and its theoretical models. This will be used as the theoretical basis for approaching the core of this study.

2.1 Definitions and notions about surveillance and privacy

2.1.1 Surveillance

A researcher can meet several definitions, notions and references of the word 'surveillance' looking up the literature, and for the scope of this study we have chosen a few, focusing on the technological aspect mostly.

Surveillance in general is

- "The monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. [8] This can include observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls); and it can refer to simple, relatively no- or low-technology methods such as human intelligence agents and postal interception."
- The word *surveillance* comes from a French phrase for "watching over" ("*sur*" means "from above" and "*veiller*" means "to watch").

Computer Surveillance is

- "The systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'. That term, a variation

of surveillance, emphasizes the systems in the investigation or monitoring of the actions or communications of one or more persons". [9]

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet.[10] But there are other sources as well: wired telephones, surveillance cameras, social network analysis, biometric and aerial surveillance, data mining and profiling, corporate surveillance, RFID and geolocation devices, satellite imagery, GPS and of course mobile phones.

Internet surveillance is the monitoring of Internet data traffic for information useful to government authorities. Because the volume of information passing through the Internet is large, surveillance generally requires a software component that scans for selected patterns of text, speech, addressing, or usage, and which flags items of interest for inspection by a human operator. Targeted content for online surveillance may be illegal (e.g., child pornography), politically suspect (e.g., human-rights websites accessed by citizens living under authoritarian regimes), or evidential (e.g., e-mails or voice messages exchanged by suspects).

To conclude with definitions, this is the way to express the word "surveillance" if we examine a set of activities that have a similar characteristic:

"Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance". [11]

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. However, many civil rights and privacy groups, such as the Electronic Frontier Foundation and American Civil Liberties Union, have expressed concern that by allowing continual increases in government surveillance of citizens we will end up in a mass *surveillance society*, with extremely limited, or non-existent political and/or personal freedoms. Fears such as this have led to numerous lawsuits. [12]

2.1.2 Information Privacy and relation to surveillance

Personal information privacy is defined as "the ability of the individual to personally control Information about one's self. [13]

Internet privacy refers to “the right of Internet users to conceal their personal information and have some degree of control over the use of personal information disclosed to others” (Rezgui et al., 2003) [14]

As stated by professor of Law Dr. Bygrave in a Constitution Committee of the house of Lords in UK, “Surveillance, by its very definition, involves a reduction of privacy”.[15]

On our point of view, electronic information privacy actually disappeared when the first computer network was created. And things are getting worse ever since, in the sense that surveillance has increased exponentially.

2.2 Surveillance Society

The steadily increasing significance of information and communication is inherent with the rise of a *surveillance society.* This term is met in numerous articles, papers, books and scientific research and is extremely up-to-date in a media point of view because of last summer headlines about the NSA scandal. The vast majority of the last three months people’s reactions shows that individual users of every type of digital communication system need to take as much as possible action in order to break this involuntary embracement with modern “Big Brothers”.

Surveillance can be thought of as an attempt by the dominant stakeholders of our time to expand and maintain their power by controlling all communication. Therefore, it is simple to speak of this society as a conspiracy of authoritarians and cyber dictators.

The concept of surveillance as a means of preserving and enlarging power by the establishment via the manipulation of communication is not new. Neither the idea of a monitoring society or an Orwellian conspiracy. The media's focus on isolated stories of intrusion of personal privacy and their "sci-fi" representation of the global scale of surveillance displays a scary picture, nevertheless it's not so far from reality. Seldom though they take in consideration the complicated canvas that emerges from the social, ethical, political and law issues at hand. Very often when surveillance is discussed, it is done in terms of either simple cause-and-effect (‘CCTV will prevent crime’) or fear (‘we will all be under control’). We will come to Big Brother later on, but “the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy”. Surveillance may be viewed as progress towards efficient administration, in *Max*

Weber's view, a benefit for the development of Western capitalism and the modern *nation-state"*. [16]

Hence, understanding surveillance society as a product of modernity helps to *avoid two major traps*: thinking of surveillance as an evil plot weaved by totalitarian regimes *and* thinking that new technology produces surveillance. Furthermore, it is a well-known fact that lots of fanatics exist who combine those two ideas into one conspiracy theory.

In "Report on the Surveillance Society" [11] we meet the following clarification:

"But getting surveillance into another perspective as the outcome of bureaucracy and the desire for efficiency, speed, control and coordination does not mean that all is well". What the authors imply here is that the argument that "*if you have nothing to hide, you have nothing to fear*" is very misleading and dangerous. This could be justified with some very good arguments that are not a part of this study; but to give an idea, once a set of rules for surveillance is in place, people might not agree with any future change of them to the tightest, for whatever reason. But then, it will be too late to protest, since it is usually not the people who decide about those changes of policies.

In an extreme example, Cardinal Richelieu[2] understood the value of surveillance when he famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged."

Also, in the information age, the idea of a single entity holding that information does not hold true. The massive pressures to share information within and beyond government mean that information is constantly on the move. Sooner or later, information held by the government will be shared across the government and with the private sector.

Finally, nation states can seek to dominate or manipulate international or private organisations that supply information products or which regulate information infrastructures. As seen above, the American NSA has established a working relationship with many of the major software and hardware companies, and through these relationships has ensured that encryption systems within export versions of software in particular are less sophisticated than US internal market versions, and are *more easily crackable*.

---

[2] Armand Jean du Plessis, Cardinal-Duc de Richelieu et de Fronsac (1585 – 1642) was a French clergyman, noble, and statesman

The GCHQ and NSA also work with the International Licensed Cable companies (ILC) to be enabled to more interception. The NSA has reportedly many representatives working on transnational standardization committees, particularly with the MFA Forum (which is an unaccountable international body, responsible for developing of common data transfer standards. It consists of all of the major information and telecommunication companies from all the industrialized nations).

Also, there are usually multiple agencies or freelance agents called “Data brokers”, which are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies [17]

These agents have their personal databases and are subject to both commercial and government pressures to sell or purchase them, regarding anti-fraud, anti-terrorist, and law enforcement needs.

According to law in many countries, the citizens have the right to know how their information is being used and what information is held about them. However, there are a few exceptions to this requirement. There is a *data controller* who provides the citizens the information on all of the data that is held about them and all details of processing them. This is some manner allows to rectify the power of the asymmetry of surveillance. Especially when consent to utilize the personal data of an individual has been obtained, rather than literally granted. The problem is that many people do not know about the rights their country has to offer, so they fail to exercise them and receive very little assistance from others throughout this process.

To conclude with this context, users’ personal data are under a continuous attack of collection, manipulation and use, often without limits and respect. The individual rights are constantly violated, in an increasingly wide-ranging fashion. In his book “1984” George Orwell has forecasted that “those who will have the ability to manipulate our information and our data, will have the authority and will oppress us, whether we like it or not”.

2.2.1 Facts about surveillance and privacy

In the next paragraph we will see some numerical facts that help us understand the magnitude, the quality of privacy violation and some of its reasons.

- From 1979 till 2012 the Foreign Intelligence Surveillance Act (US law which prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" Court) has approved 33,942 cases of surveillance and disapproved 11! [3]
- On December 31, 2012, a Special Source Operations NSA official wrote that ShellTrumpet program had just "processed its One Trillionth metadata record".[4]
- 68% of Facebook users do not understand Facebook's privacy settings [5]
  69% of internet users believe they have less control over their data than they did 5 years ago. Despite this, only 28% of people consider privacy more important now. Not surprisingly, avid social media users are less concerned about privacy than social media non-users (20% versus 58%)[6]
- Roughly one in five people have never changed the privacy settings on their social media accounts, *not ever*[7].
- Almost a quarter of adults (24%) said they feel they have little to no control over the personal information they intentionally share online through retail transactions, email, or social media. Moreover, nearly half of U.S. adults surveyed (45%) feel they have little or no control over the personal information companies gather from them online.[8]
- When your online identity is stolen, you can develop problems with your bank and even the police. 12,000 Canadians had their identities stolen in 2005. [9]
- 43% of internet users claim that more personal data have been asked from then than necessary[10].

---

[3] Infographic from http://www.whocalledmyphone.net/wire-tapping/ June 2013
[4] From http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection
[5] Infographic by MDG Advertising, 2013
[6] report by MSNBC and the Ponemon institute, 2011
[7] Harris interactive Poll , 14 Nov 2013
[8] Trustworthy Computing | Data Privacy Day Privacy Survey 2013 Executive Summary conducted for Microsoft by Ipsos MediaCT - https://www.microsoft.com/privacy/dpd/default.aspx
[9] Phone Busters National Call Centre of Canada
[10] 2011 European Commission survey

- "It happened with the release by the Guardian about Prism, we started seeing an increase right when the story broke, before we were covered in the press. From serving 1.7 million searches a day at the start of June, it hit 3 million within a fortnight."[11] DuckDuckGo saw usage jump to 4 million daily searches on October 2013.

2.2.2 Metadata

The Guardian defines metadata within the context of technology and the PRISM scandal as follows:

"*Metadata* is information generated as you use technology…" "…Examples include the date and time you called somebody or the location from which you last accessed your email. The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place."

Fig. 1 from http://www.theguardian.com/ [18]


```
{
  "created_at": "Mon Jun 10 21:09:19 +0000 2013",
  "id": 344199622916448260,
  "id_str": "344199622916448256",
  "text": "Need to catch up? Our complete #NSAFiles coverage is here: http://t.co/iZPkknopxk",
  "source": "<a href="http://www.socialflow.com" rel="nofollow">SocialFlow</a>",
  "truncated": false,
  "user": {
    "id": 16042794,
    "id_str": "16042794",
    "name": "GuardianUS",
    "screen_name": "GuardianUS",
    "location": "New York",
    "description": "Featuring the Guardian's US coverage, conversations and reporters.",
    "url": "http://t.co/eqPigNUSme",
    "protected": false,
    "followers_count": 55597,
    "friends_count": 509,
    "listed_count": 2414,
    "created_at": "Fri Aug 29 14:52:08 +0000 2008",
    "favourites_count": 860,
    "utc_offset": -18000,
    "time_zone": "Eastern Time (US & Canada)",
    "geo_enabled": true,
    "verified": true,
    "statuses_count": 41567,
    "lang": "en",
    "contributors_enabled": false,
    "is_translator": false,
    "profile_background_color": "B2AFA9",
```


This is a truncated version of the metadata of a tweet from @GuardianUS. Accessing metadata is often possible through services offered by the provider and can be retrieved in a structured format that could include raw text, XML, or in this example, JSON. An

[11] Gabriel Weinberg (founder of DuckDuckGo, the only zero tracking and fully encrypted search engine), July 2013

easy way to see some of your own metadata is by looking at your browser's history which provides information about what websites you visited and when.

Generally metadata is “data about data”, a kind of “data exhaust” or the “trail” left behind during the use of various technology tools. And they are most valuable to surveillants, because it is much easier to harvest and store (because of their small size, compared with the whole data), while they provide essential information about the target. Even if the contents of emails (or voice conversations, tweets, chats, posts etc) cannot be directly snooped, the knowledge of when, where, from whom, to whom, and how regularly such communication takes place can tell an adversary a lot, and is a powerful tool in the wrong hands (almost anybody), as we will see in the next section..

2.3 PRISM and other surveillance programs

2.3.1 PRISM

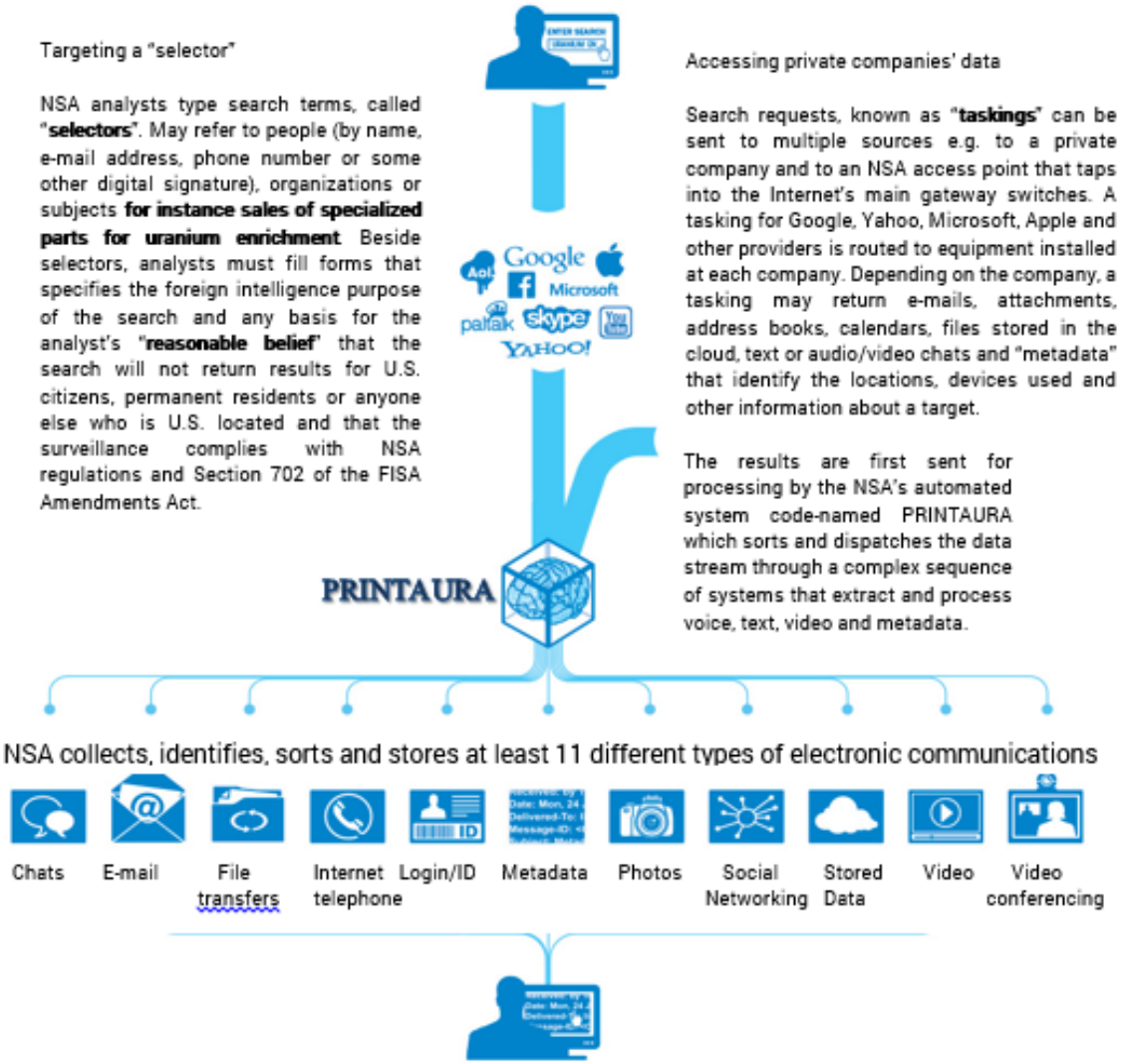
PRISM stands for “Planning Tool for Resource Integration, Synchronization, and Management”.

The PRISM allows the NSA to collect data (email, voice & video chat, videos, photos, stored data, online social networking details, among others) of foreigner users of popular Google, Yahoo, Facebook, Apple and other companies’ services. The disclosure of this belong to the *Guardian* and the *Washington Post,* who obtained sections of a classified presentation of the program, aided by “whistleblower” Ed Snowden in June 2013, 6 years after the data collection started.

The companies named in that secret presentation have denied their participation in the program. For instance this is Google's statement, given to the press: *"Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a back door for the government to access private user data”*. However, the law accordance reference leaves open areas for discussion and guessing.

Very few details are known yet about the technicalities of the program. So far we don't know if the NSA forced the companies to install a backdoor in their software or if an API is used. So far, companies denied both theories.

In the next page we see a graphic that explains to an extent some of the PRISM program functionalities, together with some inside terminology (NSA's parlance regarding the program's entities).[19]



Most metadata are collected in programs other than PRISM. For example "*Upstream*" intercepts upon the biggest junctions of internet and telephone networks or directly from telephone companies (AT&T, Verizon and Sprint).

If a target turns out to be an American or a US located, NSA calls the collection "inadvertent" and usually destroys the results. If the target is foreign but the search results include U.S. communications, the NSA calls this "incidental" collection and generally keeps the U.S. content for five years. If it believes there is evidence of a crime or that the identities are essential NSA discloses the identities to other agencies. [18]

Fig 2 Graphic: How the PRISM program works[12]

[12] Based on http://apps.washingtonpost.com/g/page/national/inner-work

2.3.2 XkeyScore and Bullrun

XKeyscore

XkeyScore is a top secret NSA surveillance program that complements PRISM (was also revealed by Edward Snowden through the 41-page PowerPoint presentation on June 6 2013). On July 31 2013, The Guardian published an article by Glenn Greenwald about Xkeyscore [20]. It is described as "a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has already collected using other methods".

On this article, Xkeyscore is analyzed and presented with the aid of some of the leaked slides. The top conclusion is that this program "allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals".

Quoting Ed Snowden, "I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email". (Fig.3 below)

US officials denied this claim, but training materials for XKeyscore show how analysts can use this, among other systems, to mine enormous agency databases. Those requests came through without the need of any court or NSA personnel review before processing.

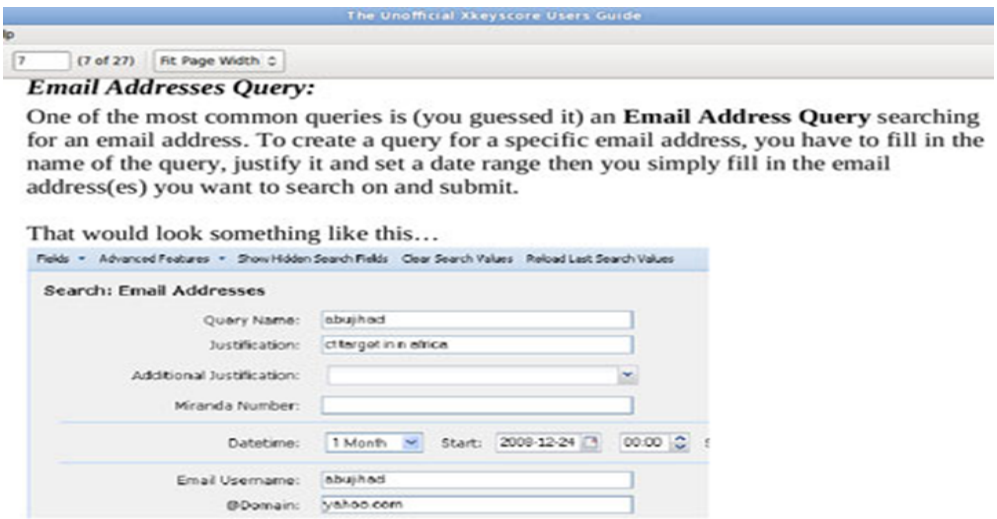


Fig. 3 XkeyScore Email search form[20]

Xkeyscore does what NSA calls *Digital Network Intelligence* (DNI). The slide in the next figure x.x.x validates that the program covers "nearly everything a typical user does on the internet", with the example of a facebook chat monitoring.

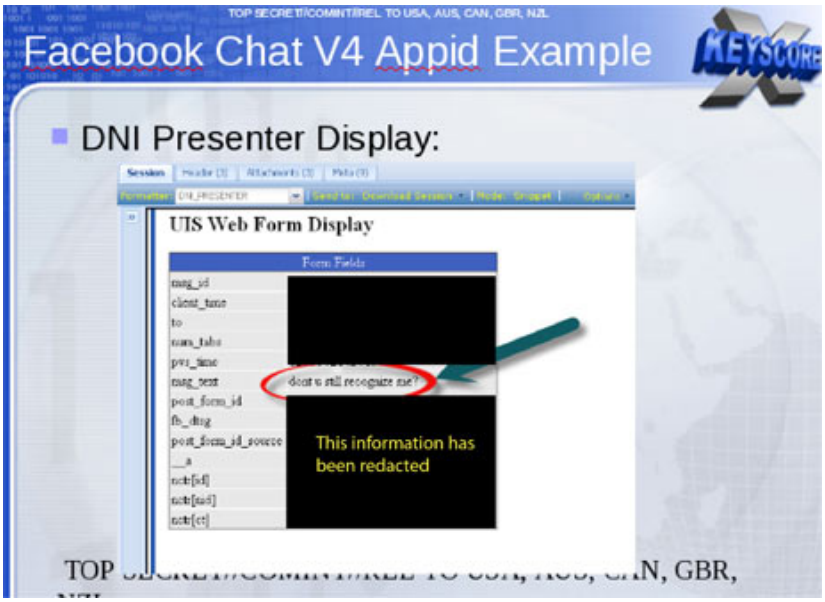


Fig.4 Analysts can monitor Facebook chats by entering use name and date range into a simple search screen.[20]

Another training slide in Fig. 5 illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.

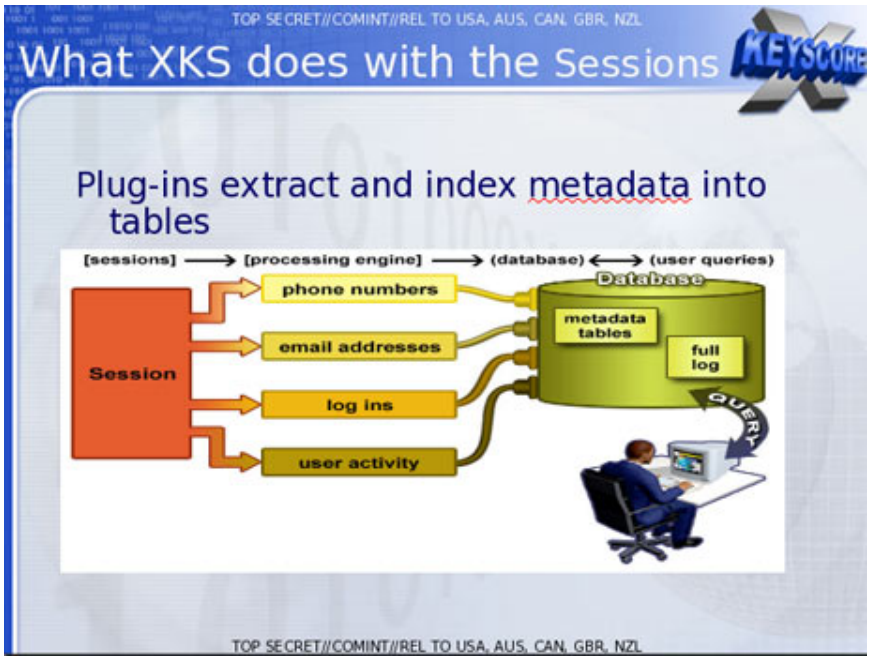


Fig. 5 Data collection session [20]

The purpose of the whole system is to allow for analysts to not only search email content, but metadata also, together with other online activities like browser history, even in the case that no known email account -named "*selector*" in NSA jargon- is

coupled with the targeted individual. The search can also be performed by name, tel. number, IP address, keywords and even the language of the user activity.

An interesting example of a selector search is shown on the next slide:

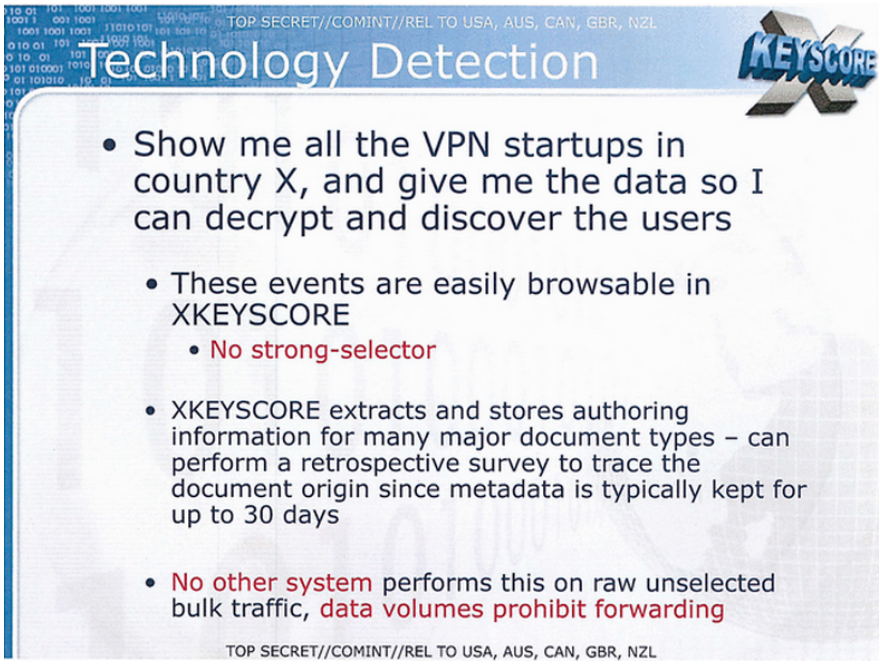


Fig. 6 Technology detection example[20]

That non-stop system is collecting so much internet data that it can be stored for three to five days at a maximum, while metadata are stored for 30 days. As a document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."[20]

According to a 2007 NSA report, the size of communications accessible through XKeyscore is amazingly large:

- 850 billion "call events" are collected and stored in the NSA databases
- This is equivalent to 150billion internet records
- Each day 1-2 billion records were added.

In total, experts estimate that today NSA can store in its new data-storage center in Bluffdale, Utah an amount of data that reaches Exabytes or Zetabytes.[13]

The ubiquity of the whole system is also very impressive, as shown in the next slide. (Notice the red dots aligned to the Antarctica!).

[13] 1 Exabyte = 10^6 Terabytes, the same as 250 million DVDs in capacity. Zetabyte is 1000 times larger

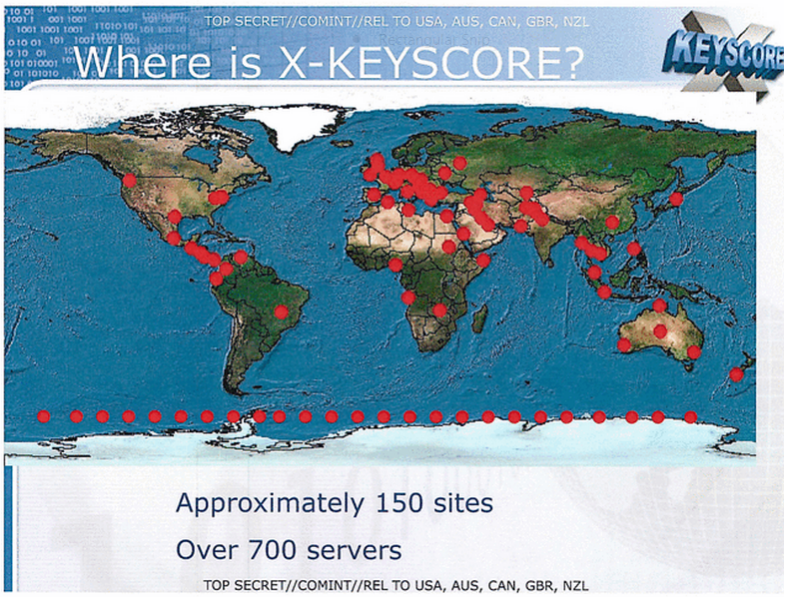


Fig. 7 Areas of deployment of XkeyScore infrastructure[20]

Bullrun

Bullrun is the codename for NSA's highly classified decryption program. It is dealing with defeating encryption used in sensitive network communication technologies like HTTPS, Voip and SSL which are used to protect shopping and banking online.

According to a New York Times article of September 2013, NSA is "working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break."[21].

The SIGINT enabling project, as a part of Bullrun program, is lobbying with encryption technology companies for encryption standards that the agency can crack.

The following excerpt from a 2013 $250 million budget proposal (also leaked by Edward Snowden) shows some methods used to weaken public used encryption.

Fig. 8 Excerpt from Bullrun budget proposal

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

(TS//SI//REL TO USA, FVEY) This Project supports the Comprehensive National Cybersecurity Initiative (CNCI) by investing in corporate partnerships and providing new access to intelligence sources, reducing collection and exploitation costs of existing sources', and enabling expanded network operation and intelligence exploitation to support network defense and cyber situational awareness. This Project contains the SIGINT Enabling Sub-Project.

(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.

2.4 Surveillance on Non-American citizens

Following the research about state surveillance we notice that most if not all of the talk about the stakeholders participating involve US entities. So there is a major question that comes in mind:

Is surveillance only affecting American citizens?

The briefing note of *European Union Directorate General for internal policies (Citizens' rights and constitutional affairs) of September 2013* [22] deals with this question and the answer is clearly negative.

It was only after the PRISM scandal, that Europe remembered the fact that most of the post-9-11 American surveillance activity was "primarily directed at the rest-of-the-world, and was not targeted at US citizens". The note argues that the scope of surveillance under the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA) has very strong implications on *EU data sovereignty* and the protection of its citizens' rights.

The executive summary claims that "…the US authorities have continuously disregarded the human right to privacy of non-Americans. The analysis of various surveillance programmes (Echelon, PRISM) and US national security legislation (FISA, PATRIOT and FAA) clearly indicates that surveillance activities by the US authorities are conducted without taking into account the rights of non-US citizens and residents."[22]

The briefing note first provides a historic part of US surveillance programs and then overviews their main legal gaps, loopholes and controversies and their differing consequences for the rights of American and EU citizens. Finally, it suggests some strategic options for the European Parliament (including a "European cloud"), the revoking or renegotiation of mechanisms that allow US companies to gather data from European users, and, significantly in the case of the Snowden revelations, "systematic protection and incentives for whistleblowers".

2.5 Possible countermeasures to surveillance

Privacy professionals suggested for a long time that state and corporate surveillance was ubiquitous, so there were really few solid privacy countermeasures for individuals even in the pre-Snowden era. In the circumstances of the present, with the raised interest of

the public about surveillance, a lot of privacy enhancing software for average everyday users appear. We reckon that even the most simple, merely informational approaches which come in the form of addons of popular web browsers contribute to this goal; the users start getting *aware* and this is the first step towards countering the problem.

Of course, this alone is not enough. Even totally aware of privacy violation users have to raise their efforts to a maximum, to reach the level of knowledge needed to secure themselves. This is not feasible in most cases, or would need professional help and knowhow, thus becoming impractical in real life.

But along with the pervasive surveillance comes a number of community software tools, developed lately (or in most of cases updated to the new reality) that can help many users that don't rank high in technology knowledge. New friendly user interfaces, providing only the necessary options succeed on this cause.

It is beyond doubt that we are in the very start of this new phase and that true privacy still needs a combination of very high technical competence and effort. However, there are some new startups that are still in the design process, promising that they will raise privacy for simple users. The currently more promising attempts met are John McAfee's D-Central router, Hemlis encrypted messaging application and Dark Mail Alliance secure email service.

2.5.1 D-Central

McAfee D-Central, a currently under design and fundraising project, will be a pocket-sized, personal router device, used to create encrypted wireless networks extending in range to a few city blocks or 800m in open space. It will provide anonymity by not being connected to the Internet and will be a building block for isolated MAN type of networks that can connect to each another without the risk of snooping by Internet service providers.

Users on each router will be able to communicate each other in either public or private, anonymous modes.

The product is announced for March 23 2014 release. It will cost under 100$ and will be compatible with Android, iPhone and PC platforms.

2.5.2 Hemlis

Hemlis (means secret in Swedish) is an encrypted messaging application. It is also in the design and crowdfunding[14] phase. The application is designed in a modern, user friendly UI to be encrypted on both ends (sender-receiver), so that neither its providers nor ISPs (or anybody else above) could have access to the messages exchanged. It is scheduled to run on Android and iPhone platforms and does not yet have a release day.

2.5.3 Dark Mail Alliance

Resurfaced from their sudden shutdown in last August, two flagship US companies, (for their struggle against email surveillance) *Lavabit*[15] and *Silent Mail* announced they join forces into a new "Dark Mail Alliance"[23]. Its goal is to build a new kind of secure email service that will encrypt the emails, rendering any monitoring nearly impossible.

The project includes a new open source tool that aims to achieve end to end encryption of any email service. For what is known so far, this new technology will be based on an instant messaging protocol called SCIMP, which saves the key code into the email for a very short time and practically deletes the email just after the user reads it. It will be used as an add-on of a normal email interface (inbox, sent mail and draft folder), which encrypts the transfer of the message, with the consent of the email service provider.

The differences between this approach and any other known email encryption (mostly based on PGP) is that Dark Mail will also prevent collection of the *metadata* of the emails and also it promises a very high ease of use, contrary to the criticized to be very hard to implement PGP.

There is no launch date specified yet, but the cryptologists of the Dark Mail Alliance claim that the product could be available somewhere in the second quarter of 2014, and they plan for IOS and Android app availability, as well as desktop version for Windows and Mac. The designers' ambition reaches to the extent that after 3-4 years this project will become something like email 3.0, meaning that most users will use email in that way.

---

[14] Coming from crown and funding, meaning fund draw from the collective effort of potential users
[15] Lavabit was Edward Snowden's secure email provider

2.6 Theoretical foundations of technology acceptance

In the following chapter we will transit from the surveillance context to a more general one; *Technology acceptance* belongs to the core of this study, meaning that the first objective, as seen in the introduction, is *to incorporate new determinants of technology acceptance in widely recognized theoretical models*. To the scope of the work, this means that we are going to use research on technology acceptance to get to the point that we can change or adopt more secure technologies for everyday use. The examined models, in order or the most general to the most specific are:

- Theory of Reasoned Action
- Theory of Planned Behavior
- Theory of Technology Acceptance

We are going to focus on the last one, its variants and its successors until we reach the core of the theory of this study: How can the technical skills of an individual together with his needs for privacy and ease of use affect the adoption or abortion/substitution of a technology.

2.6.1 Theory of Reasoned Action (TRA)

The *Theory of Reasoned Action (TRA)* is a model that finds its origins in the field of social psychology. This model developed by Fishbein and Ajzen (1975) defines the links between beliefs, attitudes, norms, intentions, and behaviors of individuals. According to this model, a person's behavior is determined by its behavioral intention to perform it. This intention is itself determined by the person's attitudes and his subjective norms towards the behavior. Fishbein and Ajzen define the subjective norms as "the person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein and Ajzen 1975, p.302)

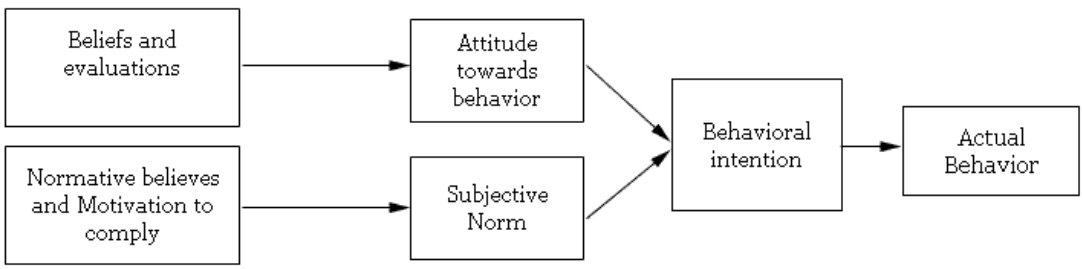


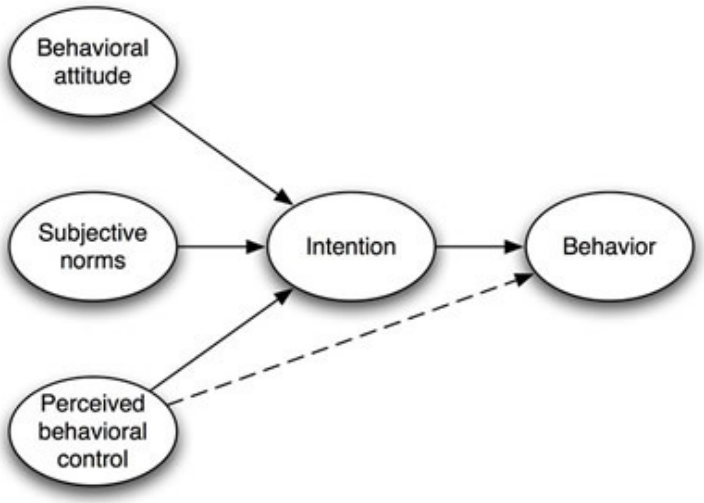
Fig.9 Theory of Reasoned Action from Davis, Bagozzi and Warshaw (1989) [24]

2.6.2 Theory of planned Behavior (TPB)

The *Theory of Planned* Behavior (TPB) evolved from the Theory of Reasoned Action. During the early 1970s the theory was revised and expanded by Ajzen and Fishbein. In 1988, the Theory of Planned Behavior (TPB) was added to the existing model of reasoned action to address the inadequacies that Ajzen and Fishbein had identified through their research using the TRA. [25]

The major difference between TRA and TPB is the addition of a third determinant of behavioral intention*, perceived behavioral control*.

Fig. 10 Theory of Planned Behavior from Isek Ajzen [25]



2.6.3 Technology acceptance model (TAM)

Among the various efforts to understand and predict the process of *user acceptance or adoption of information systems*, the TAM introduced by Davis (1986) [26], is one of the most cited theoretical frameworks. This model hypothesizes that system use is directly determined by behavioral intention to use, which is in turn influenced by users' attitudes toward using the system and the perceived usefulness of the system. Attitudes and perceived usefulness are also affected by perceived ease of use.

Perceived usefulness (PU) is defined as “the extent to which a person believes that using a system will increase his or her job performance”.

Perceived ease of use (PEOU) refers to “the degree to which a person believes that using the system will be free of effort”.

PU directly influences intention to use, while PEOU has an indirect effect through PU and attitude on the behavioral intention. The TAM has been evaluated to be not only a powerful and parsimonious model for representing the determinants of system usage, but also a valuable tool for system planning, since the system designers have some degree of control over easiness and usefulness (Taylor & Todd, 1995). *Behavioral intention* is a measure of the strength of one's willingness to exert effort while performing certain behaviors. *Attitude* explains a person's favorable or unfavorable assessment regarding the behavior in question.[27]

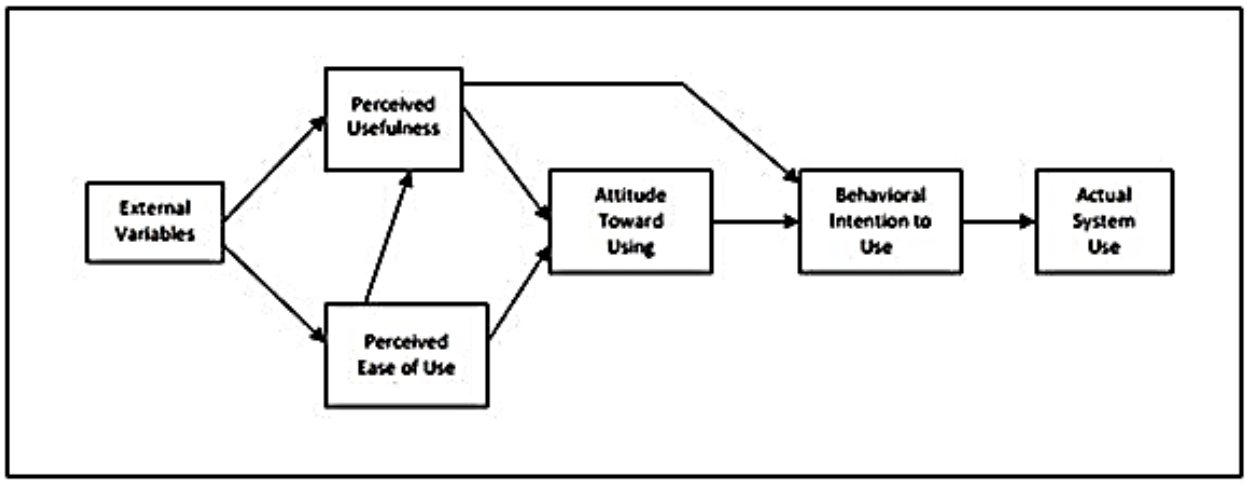


Fig. 11 Technology Acceptance Model

Counter to Fishbein and Ajzen's (1975) position, Davis (1986) and Davis et al. (1989) emphasized that PU and PEOU are people's *subjective* appraisal of *performance* and *effort*, respectively, and do not necessarily reflect objective reality.[26]

2.6.4 Some more theory based on TAM

Despite the fact that TAM is one of the most influential theories in information systems, several studies like H. Barki's "Quo Vadis TAM?" [28] have shown that despite its great scientific value, it has fulfilled its original purpose and that it is now unable as a theory to expand its core model towards the constantly evolving IS context.

Venkatesh and Davis

For that matter, Venkatesh and Davis proposed in 2000 a theoretical extension of TAM, the Unified Theory of Acceptance and Use of Technology (UAOUT) (also known as TAM2), which incorporates additional theoretical constructs spanning social influence processes (subjective norm, voluntariness, and image) and cognitive instrumental

processes (job relevance, output quality, result demonstrability, and perceived ease of use). [29]

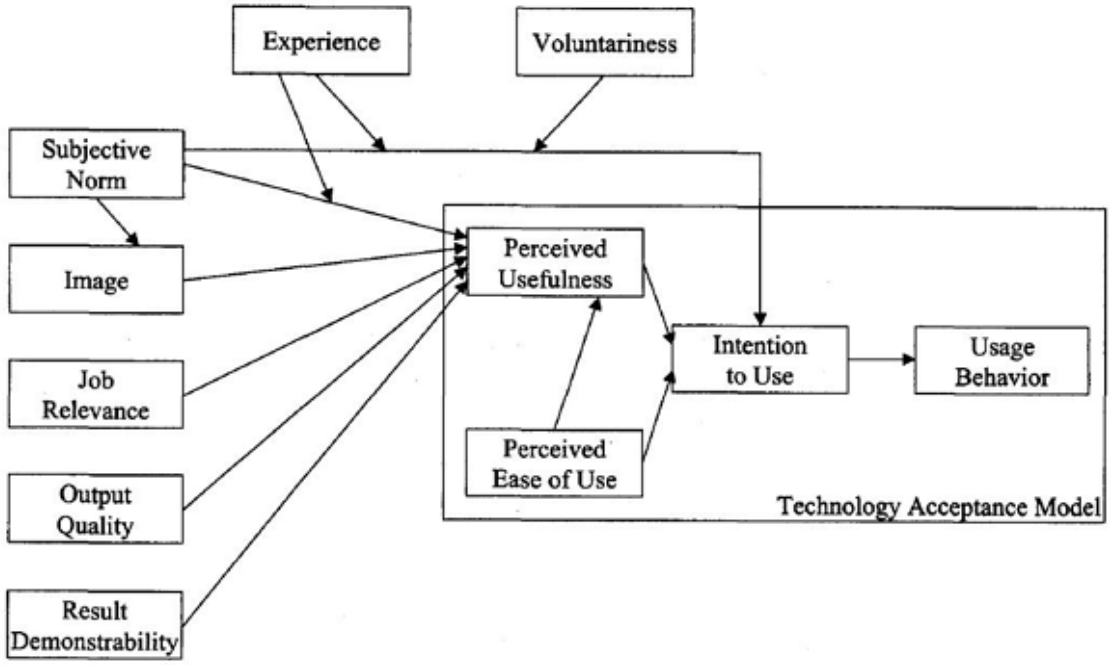


Fig. 12 Proposed TAM2—Extension of the Technology Acceptance Model

Xu-Dinev

H. Xu and T. Dinev study about empirically tested relationships for developing well-balanced policies of security protection and civil liberties [30] analyses the notions of Security-Liberty balance through two constructs:

(a) *Perceived Need for Government Surveillance* as the *positive* element ensuring protection and

(b) *Reliability Government Intrusion Concerns* as the *negative* element reflecting citizens' concerns about the government's use of personal information.

They also define *internet self-efficacy* as "an individual's belief in his or her own capability to use the internet and various internet-related applications to accomplish various online activities" and *social awareness* is defined as "the citizens' behaviors with respect to following and being actively involved in communities' and government policies and initiatives, including those related to the technology and internet". Using those constructs they build the following theoretical model of their study:

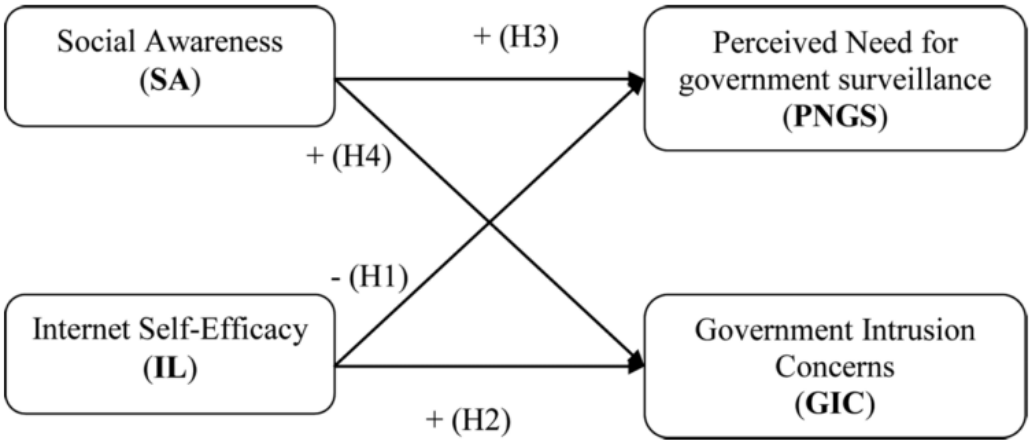


Fig. 13 Xu-Dinev theoretical model [30]

We notice that Social awareness (SA) and Internet Self Efficacy (IL) affect positively the Government Intrusion Concerns and that IL affects negatively the Perceived Need for Government surveillance. We will adopt this conclusion for our study.

V.Katos

On his 2011 empirical study V. Katos [31] states that "more research is needed to illuminate the mechanism through which *information privacy* influences actual *online transactions"*. He proposes and empirically validates an integrative framework of online transactions at the individual level by adapting information privacy concerns and trust-risk-subjective norm beliefs and relating them to attitudes of individuals. Some of the variables used in this analysis seem to suit very well with the research needed for the objectives of this study.

2.6.5 Need for a new conceptual model

From what we have seen so far, the key findings of the literature review point to the direction of enhancements on the widely approved conceptual models of technology acceptance, ie TAM and its variants. There are many researchers who put their own perspective on the context, depending on the subject; but despite that, they all agree that TAM serves very well as a base and although already 25 years have passed since its first publication, it is still on top of academic interest. On the next chapter we will try to build an extension of these models, based on previous findings and connecting them with the urgency to raise awareness about endangered privacies.

3 Problem definition and architecture

In this chapter we are going to define and explain the problem that this thesis will try to tackle. Following this, we will revisit the TAM theoretical model, altering its basic variables and using our own scheme. The new variables will be described and analyzed theoretically leading to a draft representation, in the form of tables, of the relations between them as a product of this phase. Next in line is describing some parts of implementation methodology. Summing this chapter we will have the basic components to start designing our system.

3.1 The problem of privacy violation

This thesis is dealing with the problem of electronic surveillance and how a user can counter the effects of this by applying some privacy oriented changes to his everyday use of technology.

As stated in the introduction, the goal is to propose some action towards helping users decide how their "use of technology" habits should change. We have well crossed over the "Ignorance is a Bliss" line. That means that given all the latest facts (§1, §2.2-2.3), plus research found on literature, it should be now clear that some –so far unknown- degree of effort must be applied to the privacy-versus-ease of use balance scale; some of the most important aspects of the problem are listed below":

- If someone has an online presence of any kind in 2013, he has to be aware of the dangers and implications about his personal data and life in general
- More privacy applied to this online presence usually leads to a more complex and unfriendly user experience
- That means that most of the tools that offer *significant* security (i.e. encryption of personal files and/or encryption of the communication channels) against surveillance, either state or corporate or the *new hybrid sort recently revealed*, are almost impossible to apply for the typical internet user

- ❖ This also mean that we are already starting to draw the picture of the extension determinants: Ease of use, privacy and technical competence have to be applied in some way as variables to influence technology adoption (or discard/substitution of some technology)
- ❖ Having said all of the above, the tradeoff between security and ease of use should be seen with a practical manner, so that *action* can be carried out relatively fast

We will come later on this, but for now we should keep in mind that for the scope of this study we will focus on the *human* type of security of IS (as seen on fig. 14 below). Of course, also *network* and *message* security must be applied, but mostly *as a result of a whole new attitude regarding privacy* and less as ad hoc categories.

The following table shows the four different types of security that should be considered:

Security overview

Type of security	What is it?	When is it useful?
Human	Simple changes you can make to your **behavior.**	Helps prevent human error from being the **weak link** in any security system.
Device	Steps to make your **computer or phone** less vulnerable to attack.	Useful whenever your device might **physically** fall into the hands of an attacker.
Message	Ways to encrypt **individual messages** you send and receive.	Required if you want to ensure the **confidentiality** of a particular message while stored and transmitted.
Network	Blocking sites that track you and encrypting your **internet traffic.**	Helps protect against behavioral tracking, account hijacking, censorship, social network mapping, eavesdropping, and advertising.

Fig. 14 [https://help.riseup.net/en/security] [32]

As we seen on previous chapters, network surveillance is widespread; so, *network* security is a social problem that constantly affects everybody. On the contrary, *device and message* security are important only for people who are being targeted individually.

However, the most important and difficult to achieve is the *Human* type of security. This implies that the individual user is totally aware of the problem and is willing to

change his technology habits. But, even though privacy among naive users means just "leave me alone" and "don't spook around me", only a tiny minority of them is capable of self-defense against surveillance. Without assistance, most are simply incapable of self-protection and they do need support, either by a specialist or, as this thesis will try to implement, via a form of automated guidance (wizard).

3.2 Modifying TAM

Revisiting the basic TAM picture we will stand on the subset of PEOU and PU that leads to the Intention to use and the actual use of a privacy technology.

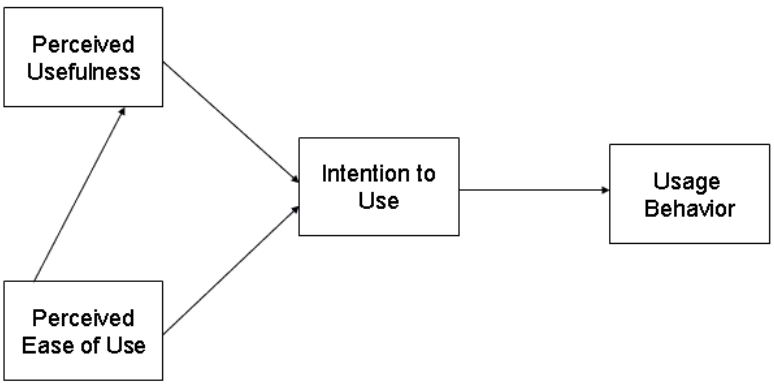


Fig 15 TAM Basic representation[26]

For the context of this study, we will have to incorporate 2 more constructs, namely (1) *Need for Privacy* (PRIV) and (2) *Level of Technical Competence* (LTC).

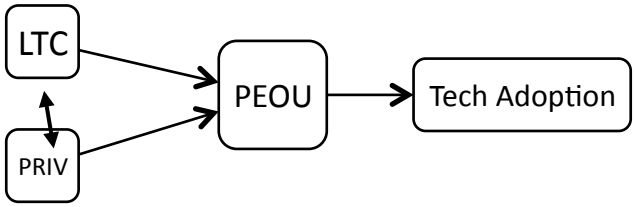
The (1) is a variable that depends on a lot of antecedents met in studies mentioned previously on §2.4, like social awareness, government intrusion concerns, (Xu and Dinev), in the sense that one must be informed and worried about that latest developments on -whatever kind of- surveillance. It is not easily defined and measured, so more work has to be done to examine it properly.

The (2) is a variable which can be measured by a number of questions regarding an individual's level of knowledge about technological aspects of his life, mostly referring to computers, internet, networks etc. It resembles somehow internet self-efficacy (met in research earlier). This set of questions may span from simple everyday tech problems up to security-related questions about the use of personal data in social networks and –at an extreme fashion- about ways of "totally" controlling one's digital persona (profile).

From the basic TAM scheme we are mostly interested in PEOU, since PU is outside the boundaries of this work. Also we will refer to *Intention to Use* and *Actual Use* as one

unified construct, named “Technology Adoption” for simplification. We can now draw the first attempted model like below:

Fig.16 Modified model



As in any causal relationship, every variable has to rely on some antecedent variables. In our model the antecedents of PEOU are LTC and PRIV, even if they are not independent from each other.

In this simplified scheme of fig. 16 we see that LTC and PRIV affect in some way the PEOU, which then leads to Tech Adoption. But they are also interacting between themselves in some way that has to be studied. So now we have to analyze those constructs in a concise way, to help the purpose of *constructing questions* that will be used later in our implementation.

3.2.1 Level of Technical Competence (LTC)

Initially, we will make a general assumption that “Level of Technical Competence affects positively the Need for Privacy and Perceived Ease of Use”

So how can we break down Technical Competence? It clearly relies on a person’s previous experience with technology, his habits and attitudes with the use of software and hardware and probably his studies and job background, among other things. Also we can safely assume that it *does not depend on a person’s Need for Privacy.*

As a general consideration, LTC could be characterized with one identifier as “CAN” or “KNOWHOW”.

The methodology that will be followed includes finding relevant questions that measure LTC and putting them into separate categories.

So, some general categories of questions might be:

- Capability of using *hardware* (pc, mobile phone, audiovisual equipment, electronic appliances in general etc.)
  Example: which of the following hard drive types has no moving parts?

- ❖ Capability of using *software* (of any kind, like a word processor and/or internet related applications like surfing the web, sending emails, chatting, sharing photos, videos, using social networking sites etc.)

  Example: which of the following protocols is primarily focused on the transfer of large files?
- ❖ Studies and professional experience regarding technology (degrees, training, professional skills, certifications etc.)

  Such questions are used in self-assessment surveys mostly.

3.2.2 Need for Privacy (PRIV)

First we will make a general assumption that "Need for Privacy affects *negatively* the Perceived Ease of Use" (§3.1 bullet 2).

This variable, as seen before, relies on social awareness and on concerns for government intrusion. These two elements are significantly raised at the present (§1-§2) and so is the whole Need for Privacy as a construct of our study. The fact that, as we assumed, PRIV contradicts with PEOU while LTC favors it, leads us to the conclusion that the first two variables are kind of "combating each other" in a balance kind of way; *the more privacy level needed, the more level of technical competence should be present, to achieve the same level of PEOU*.

As a general consideration, PRIV could be characterized with one identifier as "NEED".

Some categories of questions regarding privacy are listed below:

- *General* privacy attitude (what annoys a person regarding intrusion on his privacy in general)

  Example: "Would you give my home phone number to business clients?"
- *Online* privacy attitude (levels of needed privacy regarding several online activities like email, web searches, chat, social network sites etc.)

  Example: "Do you know how to lock your photos on Facebook?"
- Reaction to *Government* Intrusion(surveillance of personal data from state authority)

  Example: "Are you concerned about the power the government has to wiretap internet activities?"
- Reaction to *Corporate* Intrusion (surveillance of personal data from companies etc.)

Example: “Are you concerned about the advertising companies collecting data of your visits to websites?”

We can form privacy questionnaires potentially giving some weights (different for any question, depending on how much it affects the final LTC for any person involved).

3.2.3 Perceived Ease of Use (PEOU)

Firstly, we assume that “Perceived ease of Use *positively* affects the adoption of a technology or the substitution of a used technology”.

As a general consideration, PEOU could be characterized with one identifier as “WANT”. Although this as a word close to “NEED” that we used for PRIV, it is not the same. Generally there will be difficulty to distinguish some questions, regarding if they measure mostly the one or the other variable, because as seen before PEOU is derived by the proper mix of PRIV and LTC. But at the same time there are questions that can be arbitrarily put to measure it as a unique element.

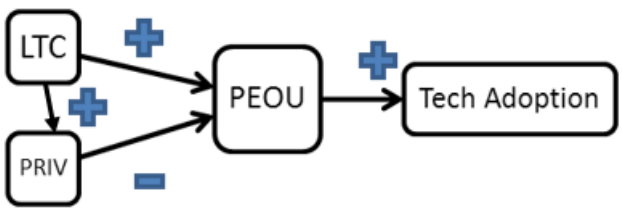
Some general questions asking only for the level of PEOU wanted could be:

- Is it easy to use?
- Is it user friendly?
- Is it effortless?
- Can I use it without written/oral instructions?
- Can I recover from mistakes quickly/easily?
- Can I use it successfully every time?

3.3 Relations of the variables

Following the definitions of the 3 basic constructs of the theoretical model that will be followed, the graph below is derived:

Fig. 17 new model shape with dependencies



Tables in fig. 18 below show the possible combinations of PRIV and PEOU, for a given LTC of a specific user. In the first case we assume that a user has the lowest possible LTC (0) and in the second that he has the top score (100). While in the first case it is yet unclear or arbitrary of how we proceed to propose tech adoption or substitution to a user, in the second case the levels of needed PRIV and wanted PEOU are irrelevant; in all combinations the user is competent enough to accept and proceed in any of the proposed tech adoption/substitution.

We will keep those cross-references for later on, when we will have more qualitative data to process. In general though, where we meet the "X", it means that there are no proposals, in the case of "OK" we can proceed to proposals, and in the case of "?" it is not yet clear. To put this in a comparison, we can define that:

- **Case X**: LTC ≤ PRIV
- **Case OK**: LTC ≥ PRIV

It must also be noted that obviously, every user would like to have the maximum possible PEOU in every case. But as the research and the modified theoretical model shows, this is only feasible in the presence of HIGH LTC, or in the case that LOW PRIV is needed.

LTC : LOW (0)			
		PRIV	
		High	*Low*
PEOU	*High*	**X**	OK
	Low	???	**X**

LTC : HIGH (100)			
		PRIV	
		High	*Low*
PEOU	*High*	OK	OK
	Low	OK	OK

Fig. 18 Relations of the variables

3.3.1 Breaking down the tables

The next step is to cut the HI and LOW values of LTC into 5 slices, each one representing one fifth of the 1-100% scale. We assign the letters A to E for respective levels of LTC, spanning from the highest level (100) to the lowest (0).

We will also cut arbitrarily the needed privacy into 3 major categories,

1. the 0-20% LOW area (where privacy matters little or none at all, has the biggest Ease of Use)
2. the 21-80% NORMAL area (where we meet the great majority of users applications)
3. the 81-100% HIGH area (where we meet only applications needing the highest privacy possible and have the *less Ease of Use*).

Filling the table is possible having in mind the cases of OK and X mentioned in the previous paragraph (where LTC ≥ or ≤ PRIV respectively). Again, "X" means that there are no proposals, "OK" means we can proceed to proposals. The gray areas in the table are those where we cannot be sure yet, and qualitative measurements should take place to help us decide whether to assign OK or X.

Now we can assign some values to the pair (Level of Technical Competence, Privacy needed) just by consulting the fig. 19 below. So for example the pair (E, 1) has the value OK and the pair (B, 3) has the value X, while we cannot set a value yet to the pairs (D, 2) (C, 2) and (B, 2).

			PRIV		
			1	2	3
			LOW 0–20%	*NORMAL 21–80%*	*HIGH 81–100%*
LTC	*E*	*0–20%*	OK	**X**	**X**
	D	*21–40%*	OK		**X**
	C	*41–60%*	OK		**X**
	B	*61–80%*	OK		**X**
	A	*81–100%*	OK	OK	OK

Fig. 19 LTC vs. Privacy

3.4 Data collection and analysis

In this chapter we will see how we can prepare the implementation of the automated system of technology proposals.

We will first try to quantify the most straightforwardly measured variable of the model, which is the LTC. There are numerous ways with online and offline tests/quizzes/exams to find out just how technology-aware a user is, like the case of COMPTIA.[33] The method of a quick online quiz is chosen here, due to the ease and the swiftness that we can collect some responses. For a solid base of data to help us measure some meaningful conclusions. So, an online quiz of mostly technical questions has to be designed.

The next step would be the study of questionnaire building techniques and elaborate mathematic analysis of the results (widely accepted scientific methods i.e. Statistical Hypotheses on theoretical models of Social Psychology and Technology Acceptance). But we consider such formal analysis to be outside the scope of the work and we will have to compromise in favor of efficiency towards the goals and objectives of this study. So, these methods needs to be addressed as future work.

Initially, the intention is to harvest some user data from some pilot quiz-like questionnaires which will try to capture the Level of Technical Competence as an independent determinant of use of technology. The format of the quiz is roughly corresponding to that of online certifications of IT professionals, only simpler, linear, with 2-3 levels of difficulty.

Following that, a score will be calculated for each user and together with other aggregated survey results, it will populate a user's database table, used later in the application.

These survey data will also be critical to find the feasible level of privacy proposals that a user can achieve.

3.4.1 Level of Technical Competence (LTC) quiz

The design of the quiz can be a quite challenging task. It can break into several categories, to extract results of LTC for many areas of IT technology, with several kinds of question sequences (called question logic). However, for the purpose of this work we will choose multiple choice questions with 4 possible choices (one of them is right and gets one point, the others get 0). We can design a quiz with 3 pages of 10 questions each, with the first page referring generally to technology using (general hardware and tech questions), the second is dedicated to operating systems and applications, and the

third has more advanced questions from all the domain of technology use, including networks and security.

A set of candidate questions could be like that:

Question: 1. what is a file?

Question: 2. JPEG is a file format commonly used when saving ___?

Question: 3. which of these disk types can store the most data?

Question: 4. which of the following video standards has the LOWEST maximum colors?

Question: 5. which of the following is used to receive a television broadcast on a computer?

Question: 6. which of the following hard drive types has no moving parts?

Question: 7. which of the following protocols is primarily focused on the transfer of large files?

Question: 8. which of the following is a secure way to access a remote network?

Question: 9. which of the following is MOST commonly used as a heat transfer medium within a computer?

Question: 10. What is Bluetooth?

----------page 1

Question: 11. What is Windows XP?

Question: 12. What is Internet Explorer?

Question: 13. The window which shows icons for things like the mouse, sound, and display is ___?

Question: 14. To add a printer you do the following:

Question: 15. You are creating a document in the latest version of Microsoft Word. You want to send the document to a friend, who has a different kind of computer from you, and doesn't have MS Word. You want your friend to be able to see as much of the document's formatting, styles, colors etc. as possible. What will you do?

Question: 16. In Linux, which command would you use to show the directory you are currently in?

Question: 17. In Linux, which command would you use to list the contents of your current directory?

Question: 18. What is the path to the home directory of a user named Ioannis in Linux?

Question: 19. What is Google Chrome?

Question: 20. Which company developed Android?

----------page 2

Question: 21. Which of the following protocols is primarily focused on the transfer of large files?

Question: 22. Which network protocol is used to send e-mail?

Question: 23. When setting up a network, which service automatically issues IP addresses?

Question: 24. Which below file extension is not a type of compressed file?

Question: 25. Which of the following is a better practice when backing up data?

Question: 26. Which of the following is not an example of real security and privacy risk?

Question: 27. Pretending to work for the IT helpdesk in order to persuade a user to reveal their password is an example of which of the following?

Question: 28. Which of the following wireless encryption technologies is the WEAKEST?

Question: 29. Which of the following passwords exemplifies the STRONGEST complexity?

Question: 30. Which of the following does full disk encryption on a laptop computer NOT protect against?

----------page 3

After the questionnaire design, we entered the questions into google forms, connected this with a google spreadsheet and start collecting the answers. The participants need only to input a name id in the beginning of the quiz.

No other kind of personal data or metadata regarding the submission is kept, besides the timestamp. Email to the users with their performance or presenting them with their score and correct/wrong answers and maybe justification can be implemented on a later phase.

After collecting enough data, a google script[16] is run on the spreadsheet to grade the responses, which produces a second tab, with the following format:

Fig. 20 Scoring spreadsheet headers

Submission time	Name	Total Points	Score(Percentage)	Question 1 points	Question 2 points	...	Question n points

From the collected data we are mostly interested about the Score, which is given in a percentage of the correct answers over all questions. Also we are going to use the Name Id later, when we want to assign the scores to a variable in the application. The Question 1-n points columns are filled with 0 for a wrong and 1 for a right answer, allowing us to collect statistics about which questions are best answered by our participants. However, since statistical analysis of each question of this quiz does not offer us any particular insight towards our objective, (how the total score of each individual correlates with his security needs), we are just presenting some of them in the appendices. On the other hand, having the scores of *each user* recorded in a percentage form (or else a value inside the [0, 1] range) allows us to rank him in the 5 categories (A to E) mentioned in Table 19 (§3.4.1 p.33). We produce this in a column next to Score with the use of a nested if spreadsheet function, so our sheet now looks like this:

	A	B	C	D	E
	Submission Time	**Please add a name for the form submissio ...**	**Total Points**	**Percent**	**Category of LTC**
	15/10/2013 12:27:03	mhtsos	25	83.33%	A
	15/10/2013 12:28:06	kotsos	22	73.33%	B
	15/10/2013 12:51:31	thanasis	30	100%	A
	15/10/2013 16:23:02	Maria	21	70%	B
	15/10/2013 13:46:36	brasidas	26	86.66%	A
	15/10/2013 14:05:25	Opap	21	70%	B
	15/10/2013 14:18:17	sdfsefd	14	46.66%	C
	15/10/2013 14:45:21	menios	6	20%	E

Fig. 21 Snip from the produced spreadsheet

[16] found in Appendix §7.1

3.4.2 Need for privacy

To measure the Need for privacy variable we have to choose some sample questions related to privacy concerns, based on the research of bibliography. In this survey we chose to put some questions like the ones met in the following table:

Question 1 I ask myself "why I am providing personal information online?"

	1	2	3	4	5	
Very frequently	○	○	○	○	○	Very rarely

Question 2 I am worried about how much information is available about me on the internet

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Question 3 I am worried about the power the government has to wiretap internet activities

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Question 4 I am concerned that my internet accounts and database information (e.g., e-mails, shopping records, tracking my internet surfing, etc.) will be more open to corporate exploitation

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

Question 5 Do you consider sites collecting data of your Internet activity without your knowledge to be a violation of privacy?

- ○ YES
- ○ NO

Question 6 Do you think that people should have the ability to use the internet completely anonymously for certain kinds of online activities?

- ○ YES
- ○ NO
- ○ I DONT KNOW

Fig. 21 Sample questions

There are 2 kinds of questions in this example, a 1-5 likert scale type, and a simple YES/NO question (a version containing an I DON'T KNOW choice also).

After collecting the results we perform the following procedure on the exported spreadsheet:

- Step 1: add all the 1 to 5 answers and divide by the number of questions to find the average
- Step 2: divide by 5 to normalize the answers to the [0 , 1] range
- Step 3: convert the YES/NO/I DON'T KNOW answers to 1, 0 , 0.5 respectively
- Step 4: add the product of step 2 to the product of step 3 and divide by 2 in this example (two question types).

- Step 5: with the use of a nested if spreadsheet function we categorize the values we found in LOW, NORMAL and HIGH.

The product of the above procedure gives us a measurement value of the PRIV variable as it was defined in §3.2.2 and 3.3.1. These findings are used next in the implementation phase.

4 Implementation

In this chapter we are going to proceed into implementing a solution to the problem of privacy violation analyzed in the text so far.

In the study phase of literature review, there was a fairly big amount of time allocated to the search of similar projects. The exploration of web and e-libraries for relative work (in the form of studies, papers, applications -either standalone or web-based*) did not yield any significant results*.

The design of an application that helps users decide on a technology adoption/substitution is a very challenging task because of its wide interdisciplinary nature; its precedent theoretical frameworks include social psychology, survey design and result analysis, some decision support theory, IT expertise to develop an application and of course all the analytic and synthetic skills to combine all the topics mentioned above.

The goal of the practical part of this dissertation is to propose existing/running/tested/ alternatives for common applications that are on stake for data privacy issues.

So to begin with we will list the proposed software solutions by related categories, explain their use, and rank them by the user level of technical competence and by the application privacy level, thus connecting them with our research variables.

Following the requirements, we will design the implementation of the front and back end. More specifically, we will use open source technologies such as Joomla CMS, which embeds the following open source server side applications:

- PHP
- MySQL
- Apache web server

4.1 Classification of privacy enhancing proposals

The technology to defend ourselves against privacy violation of our data, either it lies in our personal information systems, or it is "data on the wire" –our internet or telephone communication interception by a third party- is available for a long time, certainly long

before the latest facts. We can put user's popular activities and defensive actions in clusters like:

- Operating Systems
- Web Browsers
- Social Networks
- Email clients
- Instant Messaging clients
- Voice over Internet Protocol (VoIP)
- Wi-Fi security
- Anti-Malware
- Mobile Devices security
- Secure Deletion
- File and Disk Encryption
- Virtual Private Networks (VPN)
- Tor browsing Anonymizer

For the context of this essay it is not possible to span our research to all the topics above. The proposal procedure will have to include some basic categories of privacy enhancing practices, related to the most important and common internet applications. All of the proposed software is free and open source. Any exceptions will be noted.

At this point we have to say that the original intention was to include Operating Systems migration proposals to more secure, open source ones, at the top of the list. As shown from the introduction of the thesis and throughout most of its part, proprietary OS like Microsoft Windows, Apple OS X, IOS, Google Chrome OS, and Android cannot be trusted on privacy, being allegedly a part of PRISM surveillance program. However the facts show that we are dealing with very recent developments on this context with no solid proof about them yet, and of course the market share is still trending heavily on Windows[17]. That means that even though a multitude of modern distributions of open source OS, like GNU Linux based Ubuntu[18], Debian, Mint, Fedora, OpenSuse and others have made great leaps on user friendliness, there is still a huge gap to fill until we reach the point that the average users of technology will wholeheartedly adopt them, abandoning years of technology habits.

However, there is still a vast array of popular cross-platform applications on stake for privacy violation; so referring to operating systems can be omitted and we can as effectively deal with changing user's *general* attitude. We can examine for instance web browsers or web searches alone. Email clients form a category of its own, and so do instant messengers (chat) and VoIP applications.

---

[17]Even outdated OS like WinXP still reaches almost one third of Windows market share, as seen on http://www.neowin.net/news/windows-xp-loses-over-2-of-os-share-in-september-windows-8-makes-slight-gain

[18] Even though it is the most recognizable Linux distro, it has known exposure to Amazon ads and other data leaks

Our application list is mostly drawn from the website http://www.prism-break.org [34], which is constantly updated with new software.

In the final stage of the wizard we have to rank our proposals to enable the comparison with the users need for privacy, expressed in the PRIV variable. To help our task we will begin from the top. We will assign to the most difficult (less Ease of Use) application the top score of PRIV. Then we are going to reach on the bottom end to assign the lowest rank to the application with the less difficulty, thus needing the most Level of Technical Competence (§3).

4.1.1 Browsers and browser addons

Web Browsers

Web browsers come easily on top of popular applications. With the spread of the web 2.0 standards and modern Web Information Systems *all* of the other applications can run from within *any* browser, running within *any* OS platform under the HTTP protocol. Hence this category of the examined applications will receive more attention and occupy more space in this work.

So if we form tables including some browsers, privacy addons and possible combinations between them (based on compatibility or existence of versions - research done on September 2013) we are driven to a template like this on the next Table.

Legend: offered ✕: not offered ■: not offered at all on this OS/browser combo

OS / Programs	Windows	Mac OS	Linux	Android	IOS
Browsers					
Internet Explorer			✕	✕	✕
Firefox					
Chrome					
Safari			✕	✕	
Opera			✕		
Browser Addons	Description				
1.Adblock on:	Blocks advertisements and trackers across web with filter subscriptions				
Internet Explorer	■				
FF					Jailbreak
Chrome				✕	Jailbreak
Safari	■				
Opera					
2. HTTPS Everywhere on:	Encrypts communications from websites				
Internet Explorer	■				
FF				✕	✕
Chrome				✕	✕
Safari	■				
Opera					
3, Disconnect on:	Visualize and block invisible tracking of search and browsing history				
Internet Explorer	■				
FF				✕	✕
Chrome				✕	✕
Safari				✕	✕
Opera				✕	✕
4. Ghostery on:	Visualize and block invisible tracking of search and browsing history				
Internet Explorer					
FF					
Chrome					
Safari					
Opera					

Table: Browsers and addons per operating system
* Only if Jailbreak is applied to the IOS device

We are obviously going to assign the browsers to the lowest rank of needed privacy (PRIV), since they apply even to users that need none at all or very little privacy enhancements. These can be proposed to *everybody, regardless of their Level of Technical Competence.*

If we review the Table 22 first column we can see that indeed all those proposals are in the OK region.

			PRIV
			1
			LOW 0–20%
LTC	*E*	*0–20%*	OK
	D	*21–40%*	OK
	C	*41–60%*	OK
	B	*61–80%*	OK
	A	*81–100%*	OK

Fig. 22 Browsers LTC vs. PRIV

Firefox

We are going to propose to all users to switch to Mozilla Firefox, the well-known free, open source web browser and achieves better results when combined with the proper set of extensions (addons) and a more privacy enhanced search engine than Google, which we will see later. Available for all OS, desktop or mobile.

Users LTC Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)

Tor Browser Bundle

For the combination of "A" category users and HIGH PRIV applications, we are proposing the use of anonymizing through hidden IP address TOR browser. Can be extremely effective as it is one of the few strong practices the surveillants still cannot tackle (as seen on the next figure)

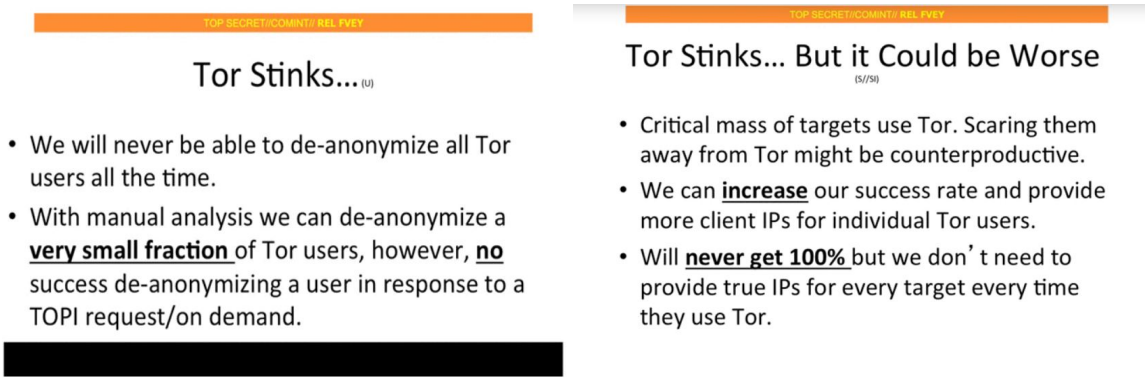


Fig. 23 Two slides from a 2007 presentation from the Guardian NSA files [35]

It lacks in speed though, due its very nature and does not work well with all sites. Also has limitations on its functionality and has to be studied thoroughly for privacy leaks. Available for Windows, Linux, Android. There is also a paid version in IOS but is still unstable.

Users LTC Rank: A PRIV Rank: 3 (HIGH)

JonDonym

Also for "A" category users, JonDo is a proxy client and will forward the traffic of your internet applications encrypted to the mix cascades and so it will hide your ip address. JonDoFox and JonDoBrowser (beta) are recommended for anonymous web surfing.

Users LTC Rank: A PRIV Rank: 3 (HIGH)

Web Browser Privacy Enhancing Addons (extensions)

Within the same context, we can assign some popular privacy addons to the second rank of PRIV. This as we can see below needs some clarification, as we don't have a value for users with LTC between 21 and 80% (categorized D, C, B). Users in category E are not eligible for suggestions of addons while users in A are.

			PRIV
			2
			NORMAL 21–80%
LTC	*E*	*0–20%*	X
	D	*21–40%*	
	C	*41–60%*	
	B	*61–80%*	
	A	*81–100%*	OK

Fig. 24 Browsers Addons LTC vs PRIV

The intuitive way to proceed is to suggest browser addons as well to the middle category of users. Of course some of them, especially of D category may not have the technical competence to understand how the proposed browser addons will help them to have more privacy. For such cases, throughout the whole mechanism of proposals, the action will be to forward the user to *study more.* With the aid of certain security oriented websites [19] and online courses we try to increase their LTC to such extent that they will

[19] Found on Appendix I

be able to understand the reasons, to install and setup on their own and enjoy the benefits.

Web browser privacy addons come in different ranks of difficulty, as follows:

Adblock

Adblock Plus and its variants and forks like Adblock Edge, block advertisements and trackers across web with filter subscriptions, thereby reducing the amount of information collected by advertisers. This is done by preventing page elements, such as advertisements, from being downloaded and displayed.

The functionality of this apply to everybody, yet the installation and/or setup and use may be difficult for the E category.

Users Rank: D, C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)

HTTPS Everywhere

This Electronic Frontier Foundation extension encrypts communications from websites. Many sites default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site. This enables the well-known hacking method called *man-in-the-middle attack* (MITM). HTTPS Everywhere fixes these problems by using a clever technology to rewrite requests to these sites to HTTPS. Applies to more advanced users and is available for Firefox and Chrome on all desktop platforms.

Users Rank: B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)

Disconnect-Ghostery

Disconnect and Ghostery are addons that visualize and block invisible tracking of search and browsing history. May apply to middle users, category C and up due to friendly interfaces. It is available for Firefox, Chrome, Safari and Opera and also as a standalone app for kids using IOS. Ghostery is also available for Internet Explorer and a standalone browser for IOS and Android.

Users Rank: C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)

Noscript

Allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice. It can be tedious so we suggest it for advanced users only and is available only for Firefox on desktop platforms.

Users Rank: A PRIV Rank: 3 (HIGH)

RequestPolicy

Increases your browsing privacy, security, and speed by giving you control over cross-site requests. For advanced users only, is available only for Firefox on desktop platforms.

Users Rank: A PRIV Rank: 3 (HIGH)

4.1.2 Web search Alternatives

Since Google, Microsoft and Yahoo are by default not privacy oriented, we have to try substituting Google, Bing and Yahoo search for alternative search providers. The use of the most prominent alternative to the browser default search engine websites, DuckDuckGo, requires some minor modifications to the web browsers search engines settings and/or optionally installation of addons, plugins and other customizations. So again we are going to assume that it applies to all user categories but the lower LTC level, E. Another reason for this is the fact that still a vast category of users believe that "Google is the internet" in the sense that, they *google* even their everyday bookmarks, or worse, even the google search page itself.[20] [36]

DuckDuckGo

DuckDuckGo is a software-as-a-service (SaaS) hosted around the world that provides the user with anonymous search results. Available through web but also available through standalone addons and apps for all major platforms.

User Rank: D, C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)

Ixquick

Ixquick is a Netherlands-based search engine which also provides the user with anonymous, encrypted web searches. It is available via web and a toolbar/search box.

Users Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)

4.1.3 Email clients and services

The most popular proprietary email services Google Gmail, Microsoft Outlook.com (ex Hotmail etc.) and Yahoo mail are reportedly being suspicious for surveillance, so we have to propose some solution to a more secure email account.

---

[20] Google.com ranks 3rd in top searches 2004-today [https://www.google.com/trends]

The same applies for proprietary email clients like Microsoft Office Outlook and Apple OS X Mail.

So the first step is to migrate to the most known email client which is candidate for this, Mozilla Thunderbird. The second step which is more difficult, is to encrypt plain text messages with PGP encryption.

4.1.4 Email clients addons

GnuPG

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications.

GnuPG comes in two flavours: 1.4.15 is the well-known and portable standalone version, whereas 2.0.22 is the enhanced and somewhat harder to build version.

Can be hard to apply for novice users, so we suggest it for the A and B categories of LTC.

User Rank B, A PRIV Rank: 3 (HIGH)

4.1.5 Generic Privacy enhancing tools

In this category we are going to assign the miscellaneous tools that cannot be categorized elsewhere. They are mostly informative and visualizing applications, either in the form of browsers addons or standalone.

Lightbeam

The most recent and impressive informative privacy addon, Lightbeam (initially known as Collusion) is a project developed by a Mozilla associate. Started actually as an experimental add-on to visualize browsing behavior and data collection on the Web. Easy to install and setup, it uses three distinct interactive graphic representations, namely Graph, Clock and List to enable the user to examine individual third parties over time and space. It is proposed to everybody mainly because of its decorative visualization, as a way to realize the relationships between the sites you visit and the third party sites that are active on those pages.

Users Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)

4.2 Development Technology: The Joomla CMS

Joomla [37] is a website content management system. It allows the administrator of a website to manage and present his content regarding to his needs. To manage the content, Joomla uses the MySQL database system and is written in PHP programming language. Also it has to cooperate with a web server, preferably Apache.

The main advantage of Joomla CMS is its extensibility. Its inner organization consists of several layers, the infrastructure which includes the libraries and the main framework, the application layer and the extensions layer. Without going deep into the system details, we can keep in mind that the application provides the necessary means for the extensions to function properly and seamlessly.

The main types of extensions are the following:

- Components: main type of extensions offering extra functionalities, appear in the main webpage space.
- Modules: smaller extensions that function outside the main page, usually of informational type, offering limited functionality
- Plugins: type of extensions that are enabled by specific events to modify the function of some component or module

For the scope of this work we are going to develop a Joomla component which we are going to name “Privacy Enhancing Wizard”.

4.3 Development core: The wizard

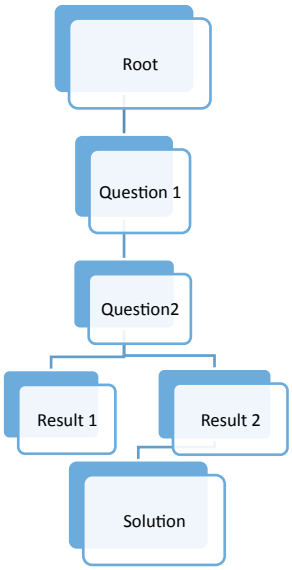
After ranking all the available software proposals, we have to design the way our wizard works, its logic, based as much as possible on our theoretical foundations. For that reason it is decided to use a scheme based on a number of steps (wizard questions and answers) that lead us to the results, which in our case are the software proposals. We are now going to describe the steps of the wizard in a top down manner.

4.3.1 Step One: The flow

The flow is the basis of our wizard. For the scope of this work we are going to produce one basic flow, called *Privacy Proposals Wizard,* test it and in the case of success we are going to produce alternatives, as we are going to see later.

Our Wizard flow is a privacy enhancing advisor, with its *questions, options, results* and *solutions*, as shown in fig. 25 below

- Questions are asked in a way that will create a 'path' or ‘tree’ that will be presented in order to be followed by the users.
- Options are the possible *answers* a user can give to proceed further on the ‘tree’.
- Results are the *software* of any kind that we can propose to the user



- Solutions are the *results* of the wizard flow, based on the users answers (options)

Fig. 25 Sample flow

4.3.2 Step Two: The questions

Designing the wizard questions is the most important part of the flow, because they lead us to the proposed solution. They have to be as explicit as possible to lead to accurate results. During the questions design phase we can also use dynamic flow, meaning we can depend our ‘path’ on previous answers.

The question might be:

Q1. “What is the online activity you are mostly concerned about:

a. Email
b. Web Browser privacy

c. Web Searches Privacy
d. Online Chat
e. VoIP Telephony and Videoconference (Skype, Google hangouts etc.)

So the options here is to route the user through a series of steps of an algorithm to answer all our questions. Depending on the users' answers, we provide him with the final solution.

In the next paragraph we are going to see an example of the procedure analyzed sofar.

4.4 Sample question flow (working example)

For a working example of this wizard we are now going to present a flow of questions that provide solutions to the problem of *Web Searches* privacy. As we have seen in our previous analysis of privacy solutions, the main candidate applications to help us enhance Web Browsing privacy are (in order of importance):

- The Web Browser itself
- Web Search engines
- Advertising blocking addons
- HTTPS encryption
- Invisible tracking of search and browsing history blocking addons
- Online scripting control
- Cross-site request control

For simplicity and presentability reasons we are going to omit the last two categories of applications for the scope of this demonstration.

Having in mind that we proposed Firefox only as a web browser (or an anonymizing alternative like TOR Browser Bundle), to replace the surveillance suspect browsers like Chrome etc, we should avoid them; but since the majority of users browse the web with all the other browsers, we are going to ask a question like "What web Browser are you currently using" and offer the option to choose them as well.

So to begin with, the *first* question is:

Question 1: "What browser do you currently use?"

Following the question we add the four options:

- Firefox
- Internet Explorer

- Chrome
- All of the major browsers (IE, FF, Chrome, Opera, Safari, etc.)

This question in terms of our wizard will be called STEP ONE.

This is shown in the next screenshot:

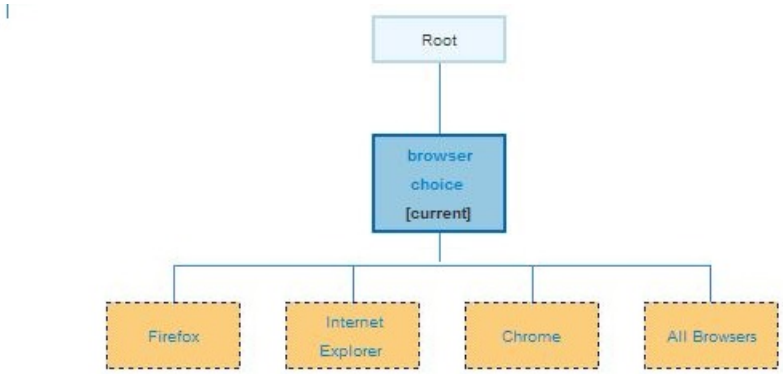


Fig. 26 Step 1 visualization

So by choosing one of the options the user we will advance to the next question.

Question 2: “Do you need to enhance your search engine privacy?”

Following the question we add the options:

- Yes, I would like a search engine that does not track my searches
- No, I do not mind tracking

This question in terms of our wizard will be called STEP TWO.

This is shown in the next screenshot:

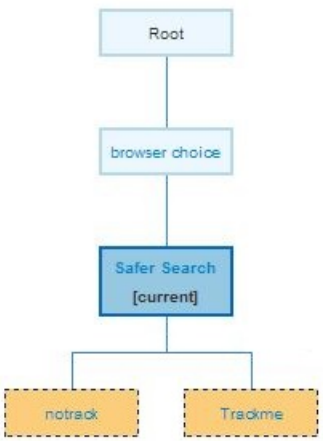


Fig. 27 Step 2 visualization

Should the user want to end the questions flow, he should press a corresponding button, or otherwise continue down the structure tree in a vertical manner.

The working example can contain more privacy related questions/steps, to expand the provided solutions list (to include more applications).

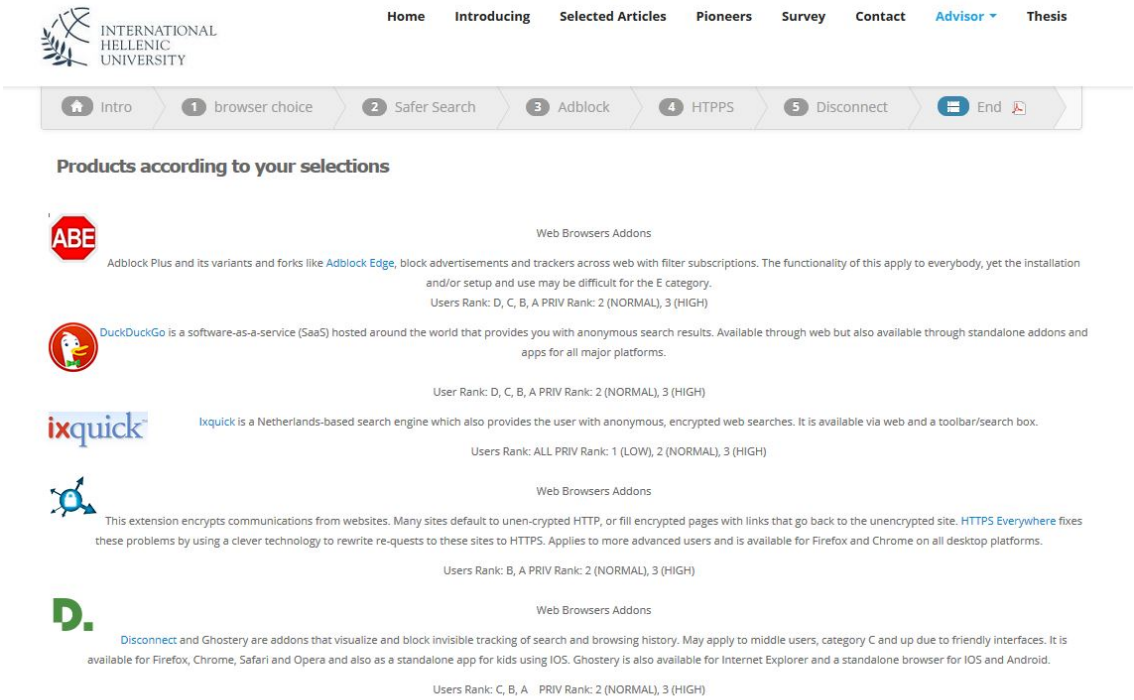
The next 3 questions will be structured under the first one, in a vertical manner as we seen already.

Question 3: “Do you need to block advertisements trackers across the web??”

Question 4: “Do you want encrypting of HTTP requests??”

Question 5: “Do you want to visualize and block invisible tracking??”

If the user chooses to select all of the conditions above to be TRUE, he reaches the end of the questions flow where he is presented with a full list of privacy enhancing



proposals according to his need/wish.

An example of this final results screen is shown in the next screenshot:

Fig. 28 Wizard final results screen

Following the results, a resume of the whole flow example is provided, so the user can review his choices that led to this solutions list.

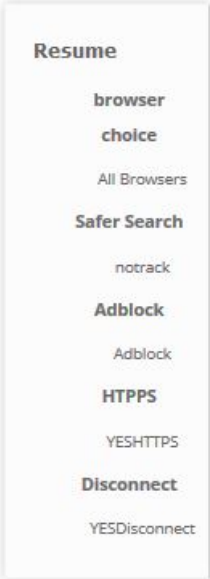


Fig. 29 The resume of the whole wizard with the chosen options

So, wrapping up, we can use the exact same procedure to ask all kinds of privacy enhancing questions, leading to proposals about the vast majority of the known applications/solutions/practices.

Since the database of applications can be constantly updated with new solutions, so can our wizard flows expand to cover all of them, thus succeeding to reach the goal of this thesis.

5 Conclusion and Future Work

5.1 Contribution and originality

This thesis contributes to the problem of electronic privacy in a variety of ways.

- First, by stating all the latest facts regarding the global surveillance, it raises awareness of the ubiquitous nature of violation of the basic human right of privacy, which has evolved in such size that no user of today's technology can be indifferent any more.
- Second, by combining the theoretical frameworks of Technology Acceptance with a simple way to reach tangible results
- Third, by recording a user's need for privacy it helps in a practical manner to bridge the gap between very advanced and typical everyday users
- Fourth, by suggesting solutions in a straightforward manner, spanning from the most trivial and obvious ones to the most advanced, depending on users technology ranking and their need for privacy.

As stated in the implementation part of this work (§4), this kind of approach has not yet been developed in a structured way in any of the usual security related sources of knowledge and/or applications. A rather extensive research, throughout the whole 4 month period of this dissertation did not meet any similar frameworks.

The findings of this work have to be interpreted considering its limitations. We have to keep in mind that it is not practically possible to incorporate all the variables of the technology acceptance and analyze them thoroughly within the framework of a single dissertation, or to fully validate them scientifically.

5.2 Personal reflection

This dissertation writing process has revealed some very important implications which were not obvious beforehand. First and most critical is that the introductory part, related to the recent surveillance outbreak, was so intriguing and consuming as a topic, that absorbed my full attention until a late stage, leaving less time to the progress towards the objectives. Second, the review of theoretical technology acceptance models was a

very demanding task, which implies a prior knowledge of social psychology evaluating methods, or a more generous time allocation, which was not available; this resulted unavoidably to a limited validation of the underlying model and as such not all assumptions were tested to the fullest possible extent.

This context was really hard to handle within the scope of a single dissertation, because of the steady flow of surveillance revelations breaking online every day, adding up to an already massive collection. But on the other hand, it is too important for the community and very stimulating as an issue to inspire the attempt.

5.3 Future improvements

Having in mind the above implications, together with the potential of this work we could foresee the following possible improvements coming as a reasonable extension for the future:

1. Better integrating of the measurement (surveys, quizzes etc.) results into the proposal wizard flows and combining them in a seamless way, possibly in a complete standalone web application (by using an alternative technology).
2. Further research and use of quantitative methodologies (using for example statistical models, null and alternative hypothesis and more) to better measure technology acceptance variables, especially the new ones proposed in this study (as explained in §3.4).
3. Research and study of the privacy enhancing proposals to the fullest possible extent, adding the new ones as soon as they appear. Those security practices include new items in the already listed categories, as well as new ad hoc applications that classify as counter-surveillance solutions.
4. Integrate (with the application mentioned in 1) links to the most acknowledged privacy practices repositories, as informational and/or practical, with indications of LTC and PRIV variables so that the user can follow and expand his privacy safeguards.
5. Incorporate a user registration system so that revisiting users can view previous results of their quiz or survey, the previous proposal scheme they were offered, and possibly another application that help them automate installations and tests of the new applications.

5.4 Conclusions

After many years of information technology development, we have reached a point where human and computer interaction has yielded some exciting results towards everyday practical matters. Unfortunately, those same results rely on a ubiquitous invasion on everybody's privacy. And if anybody wants to fully shield himself with encryption and any other anti-surveillance methods, this comes with the cost of rejecting almost all of the spectacular benefits of the new technologies.

There is plenty food for thought regarding the question "is privacy worth it?"

From what we have seen throughout his essay, countering surveillance surely includes compromises and tradeoffs towards ease of use. Keeping an acceptable privacy level *is not easy and is never guaranteed.*

It goes without saying that most users probably want to be able to facilitate their everyday digital lives, improving social needs by innovative services, sharing anything they want with friends, family and colleagues without any concerns about their data being recorded, scrutinized, judged or exploited for -any- reason. This is not likely to happen soon, but on the same time *the only way to expect some real improvement on this issue will come as a result of more users of modern technologies applying some – even elementary- efforts to enhance their online privacy.*

We hope that we demonstrated in this essay that it is totally possible and not too tedious to progress towards *improving* the individual's online privacy. As noted above, there are no guarantees of effectiveness, but on the other hand there are no reasons why one should abandon himself to both state and corporate arbitrariness.

Concluding, we will revisit a quote made by Glenn Greenwald[38]:

"The way things are supposed to work is that we're supposed to know virtually everything about what they [government] do: that's why they're called public servants. They're supposed to know virtually nothing about what we do: that's why we're called private individuals."

6 BIBLIOGRAPHY

[1] "So Just Exactly What Is NSA's Prism, More Than Reprehensibly Evil? - Falkvinge on Infopolicy." [Online]. Available: http://falkvinge.net/2013/06/08/so-just-exactly-what-is-nsas-prism-more-than-reprehensibly-evil/.

[2] "N.S.A. Able to Foil Basic Safeguards of Privacy on Web - NYTimes.com." [Online]. Available: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=1. [Accessed: 09-Sep-2013].

[3] "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video | World news | theguardian.com."[Online]. Available: http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video.

[4] A. Weiner, "Summer of 2013 Chock-Full of Scandals Snowden seen as most scandalous among headline-grabbers from Paula Deen to." p. 186, 2001.

[5] B. Schneider and D. Banisar, "The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance," *EDPACS*, vol. 25, no. 11, pp. 17–18, May 1998.

[6] J. Gilliom, "OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY," *Univ. Chicago Press*, vol. 12, no. 2, pp. 70–73, 2001.

[7] "Wiktionary." [Online]. Available: http://en.wiktionary.org/wiki/digerati. [Accessed: 05-Sep-2013].

[8] D. Lyon, *Surveillance Studies: An Overview*. 2007, p. 243.

[9] R. Clarke, "Information Technology and Dataveillance," *Commun. ACM*, vol. 31, pp. 498–512, 1988.

[10] B. W. Diffie and S. Landau, "Internet Eavesdropping : A Brave New World of Wiretapping," pp. 2–5, 2009.

[11] D. Wood, K. Ball, and D. Lyon, "A report on the surveillance society," *Surveill. Stud. ...*, no. September, 2006.

[12] "Is the U.S. Turning Into a Surveillance Society? | American Civil Liberties Union." [Online]. Available: https://www.aclu.org/technology-and-liberty/us-turning-surveillance-society. [Accessed: 11-Sep-2013].

[13] S. Stone, E.F., Gardner, D.G., Gueutal, H.G. and McClure, "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations," *J. Appl. Psychol.*, vol. 68, no. 3, pp. 459–68, 1983.

[14] A. R. A. Bouguettaya and M. Y. Eltoweissy, "Privacy on the Web: facts, challenges, and solutions," *IEEE Secur. Priv. Mag.*, vol. 1, pp. 40–49, 2003.

[15] House of Lords, "Surveillance : Citizens and the State Volume I : Report," vol. I, no. January, 2009.

[16] M. Weber, K. E. Maximilian, C. W. Mills, and H. H. Gerth, *From Max Weber: Essays in Sociology. Translated, edited and with an introduction by HH Gerth and C. Wright Mills*. Kegan Paul, 1947.

[17] GAO, "Personal Information: Agency and Reseller Adherence to Key Privacy Principles," 2006.

[18] "A Guardian guide to metadata | Technology | theguardian.com." [Online]. Available: http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1111111. [Accessed: 09-Sep-2013].

[19] "Inner workings of a top-secret spy program - The Washington Post." [Online]. Available: http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/. [Accessed: 08-Sep-2013].

[20] "XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | World news | theguardian.com."[Online]. Available: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[21] "Documents Reveal N.S.A. Campaign Against Encryption - Document - NYTimes.com." [Online]. Available: http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

[22] DIRECTORATE GENERAL FOR INTERNAL POLICIES, "The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens ' fundamental rights."

[23] "The Dark Mail Alliance Wants to Reinvent Email as We Know It." [Online]. Available: http://gizmodo.com/the-dark-mail-alliance-wants-to-reinvent-email-as-we-kn-1455074428.

[24] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Manage. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989.

[25] I. Ajzen and M. Fishbein, “Theory of reasoned action/Theory of planned behavior,” *Univ. South Florida*, vol. 2007, pp. 67–98, 1988.

[26] F. D. Davis, “Perceived Usefulness,Perceived Ease of Use, and User Acceptance of Information Technology,” *MIS Q.*, vol. 13, no. 3, pp. 319–340, 1989.

[27] N. M. Yaghoubi and E. Bahmani, “Factors Affecting the Adoption of Online Banking: An Integration of Technology Acceptance Model and Theory of Planned Behavior,” *Int. J. Bus. Manag.*, vol. 5, no. 9, p. P159, 2010.

[28] H. Barki, “Quo vadis?,” *Clin. Chem.*, vol. 59, no. 9, pp. 1423–4, Sep. 2013.

[29] V. Venkatesh and F. D. Davis, “A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies,” *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, Feb. 2000.

[30] H. Xu and T. Dinev, “The security-liberty balance: individuals’ attitudes towards internet government surveillance,” *Electron. Gov. an Int. J.*, vol. 9, no. 1, p. 46, 2012.

[31] V. Katos, “An integrated model for online transactions : illuminating the black box,” 2011.

[32] “riseup,” 2013. [Online]. Available: https://help.riseup.net/en/security.

[33] “About CompTIA.” [Online]. Available: http://certification.comptia.org/AboutCompTIA.aspx. [Accessed: 03-Oct-2013].

[34] “Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break.” [Online]. Available: http://www.prism-break.org/.

[35] “The NSA files | World news | The Guardian.” [Online]. Available: http://www.theguardian.com/world/the-nsa-files. [Accessed: 08-Nov-2013].

[36] “Google Trends - Web Search interest - Worldwide, 2004 - present.” [Online]. Available: https://www.google.com/trends/explore?hl=en-US#cmpt=q.

[37] “Joomla! The CMS Trusted By Millions for their Websites.” [Online]. Available: http://www.joomla.org/.

[38] “Glenn Greenwald (Author of With Liberty and Justice for Some).” [Online]. Available: http://www.goodreads.com/author/show/205996.Glenn_Greenwald.

[39] “Welcome to Flubaroo.” [Online]. Available: http://www.flubaroo.com/.

[40] “J3.2:Installing Joomla - Joomla! Documentation.” [Online]. Available: http://docs.joomla.org/J3.2:Installing_Joomla.

[41] “Extensions Installation | JoomlArt.” [Online]. Available: http://www.joomlart.com/documentation/other/extensions-installation.

7 Appendix

7.1 Google script for grading the quiz

The following google script is based on a free open source tool named Flubaroo [39]. It was basically designed to quickly grade and analyze assignments and was tweaked for our case to grade the responses of our LTC quiz.

```
// File: view_report.gas
// Description:
// This file contains all relevant functions for displaying the report
// viewReport: Displays the UI for grading report.
 function viewReport()
 {
   var ss = SpreadsheetApp.getActiveSpreadsheet();

   var grades_sheet = getSheetWithGrades(ss);
   if (grades_sheet == null)
     {
       Browser.msgBox(langstr("FLB_STR_NOTIFICATION"),
                      langstr("FLB_STR_CANNOT_FIND_GRADES_MSG")                                    +
langstr("FLB_STR_SHEETNAME_GRADES"),
                      Browser.Buttons.OK);
       return;
     }

   var app = createReportUI(ss, grades_sheet);
   ss.show(app);
 }

 function createReportUI(ss, grades_sheet)
 {
   var app = UiApp.createApplication().setTitle(langstr("FLB_STR_VIEW_REPORT_WINDOW_TITLE"))
                                      .setWidth("680").setHeight("490");

   var gws = new GradesWorksheet(ss, INIT_TYPE_GRADED_META);
   var points_possible = gws.getPointsPossible();
   var avg_subm_score = gws.getAverageScore();
   var num_subm = gws.getNumGradedSubmissions();

   var title = ss.getName();

   var chart_url = ScriptProperties.getProperty(SCRIPT_PROP_HISTOGRAM_URL);

   // Declare the handler that will be called when the 'Continue' or 'Cancel'
   // buttons are clicked.
   var handler = app.createServerClickHandler('emailReportHandler');
```

```
   var email_addr = Session.getActiveUser().getEmail();
   var email_addr_field = app.createHidden("email_addr", email_addr)
                               .setId("email_addr").setName("email_addr");

   var hidden_vars = app.createVerticalPanel().setVisible(false);
   hidden_vars.add(email_addr_field);
   handler.addCallbackElement(email_addr_field);

   // create the main panel to hold all content in the UI.
   var main_panel = app.createVerticalPanel()
                       .setStyleAttribute('border-spacing', '10px');

   var grid = app.createGrid(4,1).setCellSpacing(5);

   grid.setWidget(0, 0, app.createLabel(langstr("FLB_STR_GRADE_SUMMARY_TEXT_REPORT_FOR") + ': '
+ title)
                             .setStyleAttribute('textDecoration','underline'));
   grid.setWidget(1, 0, app.createLabel(langstr("FLB_STR_GRADE_SUMMARY_TEXT_POINTS_POSSIBLE") +
': ' + points_possible));
   grid.setWidget(2, 0, app.createLabel(langstr("FLB_STR_GRADE_SUMMARY_TEXT_AVERAGE_POINTS") +
': ' + avg_subm_score));
   grid.setWidget(3,                                                                    0,
app.createLabel(langstr("FLB_STR_GRADE_SUMMARY_TEXT_COUNTED_SUBMISSIONS") +  ': ' + num_subm));

   // add a top level hpanel for instructions and picture
   var hpanel = app.createHorizontalPanel()
       .setStyleAttribute('border-spacing', '10px')
       .add(app.createImage(chart_url));

   main_panel.add(grid);
   main_panel.add(hpanel);

    // add the Continue and Cancel buttons at the bottom.
   var btnGrid = app.createGrid(1, 1).setStyleAttribute('float', 'right');
   var btnSubmit = app.createButton(langstr("FLB_STR_VIEW_REPORT_BUTTON_EMAIL_ME"),handler)
                      .setId('EMAIL')

   btnGrid.setWidget(0,0,btnSubmit);
   main_panel.add(btnGrid);
   main_panel.add(hidden_vars);

   app.add(main_panel);

   return app;
 }

 function emailReportHandler(e)
 {
   var app = UiApp.getActiveApplication();
   var ss = SpreadsheetApp.getActiveSpreadsheet();
   var grades_sheet = getSheetWithGrades(ss);

   var gws = new GradesWorksheet(ss, INIT_TYPE_GRADED_META);
   var points_possible = gws.getPointsPossible();
   var avg_subm_score = gws.getAverageScore();
   var num_subm = gws.getNumGradedSubmissions();
```

```
   var title = ss.getName();

   var chart_url = ScriptProperties.getProperty(SCRIPT_PROP_HISTOGRAM_URL);
   var title = ss.getName();

   var email_address = e.parameter.email_addr;

   var msg_title = langstr("FLB_STR_GRADE_SUMMARY_TEXT_REPORT_FOR") + ": " + title;

   // form the html to email
   var html_body = '<html><body bgcolor="white">';
   html_body += '<p><b>' + langstr("FLB_STR_GRADE_SUMMARY_TEXT_REPORT_FOR") + ': <a href="' +
ss.getUrl() + '">' + title + '</a></b>';
   html_body += '</p>';
   html_body += '<table border=0 cellspacing=2>';
   html_body   +=   '<tr><td>'   +   langstr("FLB_STR_GRADE_SUMMARY_TEXT_POINTS_POSSIBLE")   +
':</td><td>' + points_possible + '</td></tr>';
   html_body += '<tr><td>' + langstr("FLB_STR_GRADE_SUMMARY_TEXT_AVERAGE_POINTS") + ':</td><td>'
+ avg_subm_score + '</td></tr>';
   html_body   +=   '<tr><td>'   +   langstr("FLB_STR_GRADE_SUMMARY_TEXT_COUNTED_SUBMISSIONS")   +
':</td><td>' + num_subm + '</td></tr>';
   html_body += '</table><br>';

   html_body += '<img src="' + chart_url + '">';

   html_body += '</body></html>';

   //email_address = Session.getActiveUser().getEmail();
   try
     {
       MailApp.sendEmail(email_address, msg_title, "",
                                {htmlBody:   html_body,   noReply:   true,   name:   "Assignment
Grader"});

       Browser.msgBox(langstr("FLB_STR_NOTIFICATION"),
                  langstr("FLB_STR_VIEW_REPORT_EMAIL_NOTIFICATION") + ': ' + email_address,
                  Browser.Buttons.OK);
     }
   catch(exception)
     {
     }

   return;
 }
```

7.2 Software installation guide

For the Privacy Enhancing Wizard to operate we have to use a full working installation of Joomla! v3.2.0, with the JA- OnePage Joomla! template.

Prerequisites that need to be met to install Joomla!:

These apply whether you have a dedicated server, a shared hosting plan server, or are installing a copy on a local computer for testing or development.

Recommended Software:

PHP (Magic Quotes GPC off) 5.4

Supported Databases:

MySQL (InnoDB support required) 5.1 or newer

Supported Web Servers:

Apache(with mod_mysql, mod_xml, and mod_zlib) 2.x or newer

Downloading and Uploading Joomla! Package Files

Download the current release of Joomla! 3.2

Move the downloaded Joomla! installation package to the server. Use a FTP Client to transfer the Joomla! 3.0 files to your server.

Creating a Database for Joomla!

Every installation of the Joomla! CMS requires a database. The database will store data such as articles, menus, categories, and users. This information is needed to make and manage your Joomla! website. Regardless of the requirements of the version, in order to install Joomla! you must have a working database, database user, database password and proper privileges for the database user.

This is a summary of the installation of Joomla! 3.2

For a full listing you must visit http://docs.joomla.org/J3.2:Installing_Joomla [40]

Installing JA One Page template for Joomla

For a full installation guide of the JA One Page template you must visit

http://www.joomlart.com/documentation/joomla-templates/ja-onepage [41]

7.3 Privacy enhancing wizard XML file

Below is the biggest part of the .xml file that contains a sample question flow of the wizard, its steps, options, products and solutions.

```
 <wizard>
  <flow>
        <id><![CDATA[11]]></id>
        <published><![CDATA[1]]></published>
        <viewresume><![CDATA[1]]></viewresume>
        <viewpdf><![CDATA[0]]></viewpdf>
        <container><![CDATA[0]]></container>
        <containerstep><![CDATA[0]]></containerstep>
        <containerwidth><![CDATA[100%]]></containerwidth>
        <containerstepwidth><![CDATA[100%]]></containerstepwidth>
        <containerstepresume><![CDATA[100px]]></containerstepresume>
        <containerheight><![CDATA[]]></containerheight>
        <title><![CDATA[ergasia2]]></title>
        <firstpage><![CDATA[<p>Welcome to our privacy enhancement wizard</p>
<p>Follow those simple steps and the wizard will guide you through our proposals</p>
<p>Click start button when you're ready.</p>]]></firstpage>
        <prehtml><![CDATA[]]></prehtml>
        <posthtml><![CDATA[]]></posthtml>
      </flow>
  <steps>
            <step>
                            <id><![CDATA[23]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <idprevstep><![CDATA[0]]></idprevstep>
                            <name><![CDATA[browser choice]]></name>
                            <precondition><![CDATA[]]></precondition>
                            <text><![CDATA[<p>What browser do you currently use?</p>]]></text>

        </step>
            <step>
                            <id><![CDATA[24]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <idprevstep><![CDATA[23]]></idprevstep>
                            <name><![CDATA[Safer Search]]></name>
                            <precondition><![CDATA[]]></precondition>
                            <text><![CDATA[<p>Do you need to enhance your search engine
privacy?</p>
<p> </p>]]></text>

        </step>
            <step>
                            <id><![CDATA[28]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <idprevstep><![CDATA[24]]></idprevstep>
                            <name><![CDATA[Adblock]]></name>
                            <precondition><![CDATA[]]></precondition>
                            <text><![CDATA[<p><span style="font-family: arial,helvetica,sans-
serif; font-size: 10pt;">Do you need to block advertisements <span style="line-height:
150%;">trackers across the web?</span></span></p>]]></text>

        </step>
            <step>
                            <id><![CDATA[29]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <idprevstep><![CDATA[28]]></idprevstep>
                            <name><![CDATA[HTPPS]]></name>
                            <precondition><![CDATA[]]></precondition>
                            <text><![CDATA[<p><span style="font-size: 10pt; line-height: 150%;
font-family: arial,helvetica,sans-serif;">Do you want encrypting of HTTP requests?</span></p>
<p> </p>]]></text>

        </step>
            <step>
                            <id><![CDATA[30]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <idprevstep><![CDATA[29]]></idprevstep>
                            <name><![CDATA[Disconnect]]></name>
                            <precondition><![CDATA[]]></precondition>
                            <text><![CDATA[<p><span style="font-size: 10pt; line-height: 150%;
font-family: arial,helvetica,sans-serif;">Do you want to visualize and block invisible
tracking?</span></p>]]></text>

        </step>
```

```
      </steps>
```

Following the steps we provide a snippet of the options

```
<options>
            <option>
                            <id><![CDATA[72]]></id>
                            <idstep><![CDATA[23]]></idstep>
                            <content><![CDATA[<p>Firefox</p>]]></content>
                            <value><![CDATA[Firefox]]></value>
                            <desc><![CDATA[Firefox]]></desc>

        </option>
            <option>
                            <id><![CDATA[73]]></id>
                            <idstep><![CDATA[23]]></idstep>
                            <content><![CDATA[<p>Internet Explorer</p>]]></content>
                            <value><![CDATA[Internet Explorer]]></value>
                            <desc><![CDATA[Internet Explorer]]></desc>

        </option>
            <option>
                            <id><![CDATA[74]]></id>
                            <idstep><![CDATA[23]]></idstep>
                            <content><![CDATA[<p>Google Chrome</p>]]></content>
                            <value><![CDATA[Chrome]]></value>
                            <desc><![CDATA[Chrome]]></desc>

        </option>
            <option>
                            <id><![CDATA[75]]></id>
                            <idstep><![CDATA[24]]></idstep>
                            <content><![CDATA[<p>Yes, I would like a search engine that does
not track my searches</p>]]></content>
                            <value><![CDATA[notrack]]></value>
                            <desc><![CDATA[notrack]]></desc>

        </option>
            <option>

.....................................
      </options>


.....................................
```

After the options we have the ‘products’ which are the privacy proposals (applications) of our working example

```
<products>
<product>
                            <id><![CDATA[105]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <order><![CDATA[6]]></order>
                            <title><![CDATA[Adblock]]></title>
                            <content><![CDATA[<p><img
src="images/ergasia/break/adblockedge.png" alt="" align="left" /></p>
<p>Web Browsers Addons</p>
<p>Adblock Plus and its variants and forks like <a href="https://addons.mozilla.org/en-
us/firefox/addon/adblock-edge/" target="_blank">Adblock Edge</a>, block advertisements and
trackers across web with filter subscriptions. The functionality of this apply to everybody, yet
the installation and/or setup and use may be difficult for the E category.<br /> Users Rank: D,
C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)</p>]]></content>

        </product>
            <product>
                            <id><![CDATA[106]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <order><![CDATA[7]]></order>
                            <title><![CDATA[Disconnect]]></title>
                            <content><![CDATA[<p><img  src="images/ergasia/break/disconnect.png"
alt="" align="left" /></p>
<p>Web Browsers Addons</p>
```

Disconnect and Ghostery are addons that visualize and block invisible tracking of search and browsing history. May apply to middle users, category C and up due to friendly interfaces. It is available for Firefox, Chrome, Safari and Opera and also as a standalone app for kids using IOS. Ghostery is also available for Internet Explorer and a standalone browser for IOS and Android.
Users Rank: C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)]]></content>

        </product>
            <product>
                        <id><![CDATA[107]]></id>
                        <idflow><![CDATA[11]]></idflow>
                        <order><![CDATA[9]]></order>
                        <title><![CDATA[Noscript]]></title>
                        <content><![CDATA[
Web Browsers Addons
Noscript allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice. For advanced users only, is available only for Firefox on desktop platforms.
Users Rank: A PRIV Rank: 3 (HIGH)]]></content>

        </product>
            <product>
                        <id><![CDATA[108]]></id>
                        <idflow><![CDATA[11]]></idflow>
                        <order><![CDATA[8]]></order>
                        <title><![CDATA[Https everywhere]]></title>
                        <content><![CDATA[
Web Browsers Addons
This extension encrypts communications from websites. Many sites default to unen-crypted HTTP, or fill encrypted pages with links that go back to the unencrypted site. HTTPS Everywhere fixes these problems by using a clever technology to rewrite re-quests to these sites to HTTPS. Applies to more advanced users and is available for Firefox and Chrome on all desktop platforms.
Users Rank: B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)]]></content>

        </product>
            <product>
                        <id><![CDATA[109]]></id>
                        <idflow><![CDATA[11]]></idflow>
                        <order><![CDATA[10]]></order>
                        <title><![CDATA[DuckDuckGO]]></title>
                        <content><![CDATA[
DuckDuckGo is a software-as-a-service (SaaS) hosted around the world that provides you with anonymous search results. Available through web but also available through standalone addons and apps for all major platforms.

User Rank: D, C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)]]></content>

        </product>
            <product>
                        <id><![CDATA[110]]></id>
                        <idflow><![CDATA[11]]></idflow>
                        <order><![CDATA[11]]></order>
                        <title><![CDATA[Ixquick]]></title>
                        <content><![CDATA[
Ixquick is a Netherlands-based search engine which also provides the user with anonymous, encrypted web searches. It is available via web and a toolbar/search box.
Users Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)]]></content>

        </product>
            <product>
                        <id><![CDATA[118]]></id>
                        <idflow><![CDATA[11]]></idflow>
                        <order><![CDATA[12]]></order>
                        <title><![CDATA[Sorry]]></title>
                        <content><![CDATA[<p>SORRY, we cant help you since you are not interested in your privacy</p>]]></content>

        </product>
            <product>

```
                            <id><![CDATA[119]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <order><![CDATA[13]]></order>
                            <title><![CDATA[NoAdsTrack]]></title>
                            <content><![CDATA[<p><img
src="images/ergasia/break/adblockedge.png" alt="" align="left" /></p>
<p>Web Browsers Addons</p>
<p>Adblock Plus and its variants and forks like <a href="https://addons.mozilla.org/en-
us/firefox/addon/adblock-edge/" target="_blank">Adblock Edge</a>, block advertisements and
trackers across web with filter subscriptions. The functionality of this apply to everybody, yet
the installation and/or setup and use may be difficult for the E category.<br /> Users Rank: D,
C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)</p>
<p><img src="images/ergasia/break/duckduckgo.png" alt="" align="left" /></p>
<p><a href="https://duckduckgo.com/" target="_blank">DuckDuckGo</a> is a software-as-a-service
(SaaS) hosted around the world that provides you with anonymous search results. Available
through web but also available through standalone addons and apps for all major platforms. <br
/><br />User Rank: D, C, B, A PRIV Rank: 2 (NORMAL), 3 (HIGH)</p>
<p><img src="images/ergasia/break/ixquick.png" alt="" align="left" /></p>
<p><a href="https://ixquick.com/">Ixquick </a>is a Netherlands-based search engine which also
provides the user with anonymous, encrypted web searches. It is available via web and a
toolbar/search box.</p>
<p>Users Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)</p>]]></content>

        </product>
            <product>
                            <id><![CDATA[120]]></id>
                            <idflow><![CDATA[11]]></idflow>
                            <order><![CDATA[14]]></order>
                            <title><![CDATA[safesearch]]></title>
                            <content><![CDATA[<p><img  src="images/ergasia/break/duckduckgo.png"
alt="" align="left" /></p>
<p><a href="https://duckduckgo.com/" target="_blank">DuckDuckGo</a> is a software-as-a-service
(SaaS) hosted around the world that provides you with anonymous search results. Available
through web but also available through standalone addons and apps for all major platforms. <br
/><br />User Rank: D, C, B, A &amp;nbsp; &amp;nbsp;&amp;nbsp; PRIV Rank: 2 (NORMAL), 3 (HIGH)</p>
<p><img src="images/ergasia/break/ixquick.png" alt="" align="left" /></p>
<p><a href="https://ixquick.com/">Ixquick </a>is a Netherlands-based search engine which also
provides the user with anonymous, encrypted web searches. It is available via web and a
toolbar/search box.</p>
<p>Users Rank: ALL PRIV Rank: 1 (LOW), 2 (NORMAL), 3 (HIGH)</p>]]></content>

        </product>
      </products>


.....
```

Finally, we have the solutions, and their options:

```
  <solutions>
            <solution>
                            <id><![CDATA[120]]></id>
                            <idproduct><![CDATA[109]]></idproduct>
                            <idhikaproduct><![CDATA[]]></idhikaproduct>
                            <idvirtueproduct><![CDATA[]]></idvirtueproduct>
                            <idjoomlaproduct><![CDATA[0]]></idjoomlaproduct>
                            <idflow><![CDATA[11]]></idflow>

        </solution>
            <solution>
                            <id><![CDATA[121]]></id>
                            <idproduct><![CDATA[110]]></idproduct>
                            <idhikaproduct><![CDATA[]]></idhikaproduct>
                            <idvirtueproduct><![CDATA[]]></idvirtueproduct>
                            <idjoomlaproduct><![CDATA[0]]></idjoomlaproduct>
                            <idflow><![CDATA[11]]></idflow>

        </solution>
            <solution>
                            <id><![CDATA[134]]></id>
                            <idproduct><![CDATA[105]]></idproduct>
                            <idhikaproduct><![CDATA[]]></idhikaproduct>
                            <idvirtueproduct><![CDATA[]]></idvirtueproduct>
                            <idjoomlaproduct><![CDATA[0]]></idjoomlaproduct>
```

```
                            <idflow><![CDATA[11]]></idflow>



        </solution>
      </solutions>
  <solutionsoptions>
            <solutionsoption>
                            <id><![CDATA[424]]></id>
                            <idsolution><![CDATA[134]]></idsolution>
                            <idstep><![CDATA[28]]></idstep>
                            <idoption><![CDATA[83]]></idoption>

        </solutionsoption>


.....................................

      </solutionsoptions>
</wizard>
```